На правах рукописи

Черников Роман Сергеевич

МОДЕЛИ И АЛГОРИТМЫ ОЦЕНКИ РАБОТОСПОСОБНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ОБЪЕКТОВ

Специальность: 2.2.15 – Системы, сети и устройства телекоммуникаций

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Владимир 2023

Работа выполнена на кафедре «Информатика и защита информации» в ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

Научный руководитель:	**Монахов Михаил Юрьевич** доктор технических наук, профессор, заведующий кафедрой информатики и защиты информации ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», г. Владимир
Официальные оппоненты:	**Надеждин Евгений Николаевич** доктор технических наук, профессор, профессор института передовых информационных технологий ФГБОУ ВО «Тульский государственный педагогический университет имени Л.Н. Толстого», г. Тула. **Малёшина Людмила Михайловна** кандидат технических наук, доцент, доцент кафедры «Информационные технологии в юридической деятельности и документационное обеспечение управления» ФГАОУ ВО «Российский университет транспорта» (МИИТ), г. Москва.
Ведущая организация:	ФГАОУ ВО «Омский государственный технический университет», г. Омск.

Защита диссертации состоится 27 сентября 2023 года в 16 часов в ауд. 301-3 на заседании диссертационного совета 24.2.281.01 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, 87, корп. 3, ВлГУ, РТиРС.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» и на сайте http://diss.vlsu.ru.

Автореферат разослан 5 июля 2023 года.

Отзывы на автореферат в двух экземплярах, заверенные печатью, просим направлять по адресу: 600000, г. Владимир, ул. Горького, 87, ВлГУ, РТиРС, ученому секретарю диссертационного совета 24.2.281.01 Самойлову А. Г.

Ученый секретарь диссертационного совета,
доктор технических наук, профессор  А. Г. Самойлов

Актуальность темы. Под работоспособностью телекоммуникационной сети (ТКС) централизованной охраны объектов (ЦОО) понимается возможность обеспечивать выполнение основных функций по передаче и обработке циркулирующей информации в заданном объеме и с необходимым качеством в условиях дестабилизирующих воздействий (ДВ). По мере развития и усложнения средств, методов и форм автоматизации процессов обработки и передачи информации в ТКС ЦОО повышается уязвимость системных процессов и ресурсов, влияющая на возможность уничтожения, блокирования или искажения информации, появления в системе «нештатных» процессов. Причинами снижения работоспособности ТКС ЦОО являются недостатки проектирования, ошибки реализации программных и аппаратных компонентов, преднамеренные информационные воздействия, ошибки операторов. Для обеспечения работоспособности ТКС ЦОО должна обладать способностью предсказывать возможные вторжения т.е. прогнозировать повышенный риск выхода из строя компонентов системы. В результате прогнозирования состояния ТКС возможно повышение защищенности компонентов. Для технической реализации данной способности в ТКС ЦОО должны быть предусмотрены средства моделирования и оценки информационной защищенности компонентов от угроз. В настоящее время существующие ТКС ЦОО такой возможностью не обладают.

Несмотря на интеграцию в ТКС современных аппаратно-программных средств защиты и управления, процессы контроля работоспособности автоматизированы лишь частично, отсутствуют эффективные модели и алгоритмы обнаружения и идентификации угроз и уязвимостей в составе единой системы. Проведенный анализ состояния информационной безопасности (ИБ) в ТКС ЦОО позволяет сделать выводы об отсутствии моделей и алгоритмов, позволяющих получать количественные оценки работоспособности ТКС ЦОО в условиях ДВ и противодействий нарушителей. Таким образом, исследования, направленные на создание моделей и алгоритмов оценки работоспособности ТКС ЦОО, актуальны и имеют практическое значение в решении проблемы обеспечения качества функционирования сетей телекоммуникаций.

Степень разработанности темы. Задачи моделирования процессов информационной защиты, охраны и безопасности в ТКС решались в трудах рос-

сийских ученых Медведковского И.Д., Зегжды П.Д., Малюка А.А., Шелупанова А.А., Ященко В.В., Петракова А.В., Соколова А.В., Макаренко С.И., Зарубина В.С., Меньших В.В., Булгакова О.М., Магауенова Р.Г., Синилова В.Г., Р. Брэтта, К. Касперски, С. Норкатта и других.

Объектом исследования диссертации является телекоммуникационная сеть централизованной охраны объектов.

Предметом исследования являются модели и алгоритмы оценки работоспособности телекоммуникационной сети в условиях дестабилизирующих воздействий.

Целью работы является разработка новых моделей и алгоритмов оценки работоспособности ТКС ЦОО. В связи с поставленной целью решались следующие **задачи** исследования:

1. Построить модель работоспособности ТКС ЦОО, позволяющую анализировать работу телекоммуникационной сети в условиях дестабилизирующих воздействий.

2. Разработать средства моделирования процессов обеспечения ИБ в ТКС ЦОО, включая базы данных угроз, уязвимостей компонентов КТС ЦОО, защитных механизмов, модель нарушителя информационной безопасности.

3. Разработать алгоритмы определения степени проявления уязвимости и силы защитных механизмов ТКС ЦОО.

4. Разработать инструментальные средства проведения аудита работоспособности ТКС ЦОО.

Научная новизна полученных в ходе исследования результатов заключается в следующем:

1. Предложена модель работоспособности ТКС ЦОО, определяемая функцией вероятностей защищенности компонентов телекоммуникационной сети на основе анализа ее инфраструктуры и условий эксплуатации.

2. Разработаны алгоритмы:

- оценки вероятности реализации угрозы при наличии уязвимости компонента ТКС ЦОО, отличающийся вновь выявленными закономерностями между типом угроз и способами проявления уязвимостей;

- оценки вероятности опасности угроз в компонентах ТКС ЦОО с учетом защитных механизмов, отличающийся вновь выявленными закономерностями между типом угроз, способом и характером действия защитных механизмов;

- определения степени проявления уязвимостей и силы защитных механизмов, выявляемых в компонентах ТКС ЦОО, оригинальность которого основана на их декомпозиции в зависимости от условий эксплуатации компонентов.

3. Усовершенствована модель оценки вероятности информационной защищенности компонента ТКС ЦОО, оригинальность которой состоит в том, что в модель включен элемент «Нарушитель» и сопутствующие ему параметры.

Положения, выносимые на защиту:

1. Синтезированные базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя и их взаимосвязи обладают универсальностью и достаточностью для ТКС ЦОО.

2. Предложенная модель работоспособности позволяет прогнозировать изменения состояния ТКС ЦОО и повышать защищенность ее компонентов.

3. Разработанные средства дают возможность снизить уровень ложных срабатываний на пульте централизованной охраны (ПЦО) на15-20%, несанкционированный доступ на защищаемый объект - на 8-10%.

Практическая значимость работы заключается в том, что предложенные в данной работе модели и алгоритмы позволяют проводить оценку защищенности информационных процессов по показателям конфиденциальности, доступности и целостности, и прогнозировать изменения состояния работоспособности структурных компонентов ТКС ЦОО для всех режимов функционирования, что позволяет выборочно применять защитные механизмы, усиливающие защищенность элементов системы.

Разработанное программное обеспечение позволяет рассчитывать вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов (св-во о гос. регистрации программы для ЭВМ №2022682661), вероятности реализации угрозы (св-во №2022680341).

Методы исследования. При проведении теоретических и экспериментальных исследований в работе использованы методы математического моделирования на основе системного анализа, в том числе многокритериального принятия решения, методы экспертного оценивания.

Соответствие паспорту специальности. Проблематика, исследованная в диссертации, соответствует областям исследований пунктов 17, 19 паспорта специальности 2.2.15 – «Системы, сети и устройства телекоммуникаций»

Достоверность и апробация. Достоверность результатов диссертацион-

ного исследования подтверждается корректным использованием математических методов, результатами вычислительных экспериментов, а также проведением пробных расчетов работоспособности ТКС ЦОО. Научно-практическая значимость работы подтверждена рецензируемыми публикациями в журналах и в сборниках научных трудов, докладами на научных конференциях. Практическая значимость работы подтверждена внедрением её результатов в обеспечение работоспособности и ИБ телекоммуникационных сетей ПЦО ОВО ВНГ и «Цербер-мониторинг», МКУ г. Владимира «Управление гражданской защиты» и администрации города Владимира, а также в инновационную научную и образовательную деятельность ВлГУ и ВЮИ ФСИН России.

Материалы диссертационной работы докладывались и обсуждались на XIII Международной научной конференции аспирантов, педагогов, молодых ученых (Москва-Иваново-Шуя, 2020), XIV Международной НТК «Перспективные технологии в средствах передачи информации, ПТСПИ-2021» (Владимир, 2021), V Международном пенитенциарном форуме «Преступление, наказание, исправление» (Рязань, 2021), III Всероссийской научной конференции «Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации» (Ставрополь, 2021), IV круглого стола ФКУ НИИИТ ФСИН России (Тверь, 2022). По результатам диссертационной работы опубликовано 13 научных работ, в том числе 2 в изданиях, рекомендованных ВАК.

Личный вклад. Все результаты, изложенные в научно-квалификационной работе, получены автором лично или при его непосредственном участии. Постановка цели и задач, обсуждение планов исследований и полученных результатов выполнены совместно с научным руководителем.

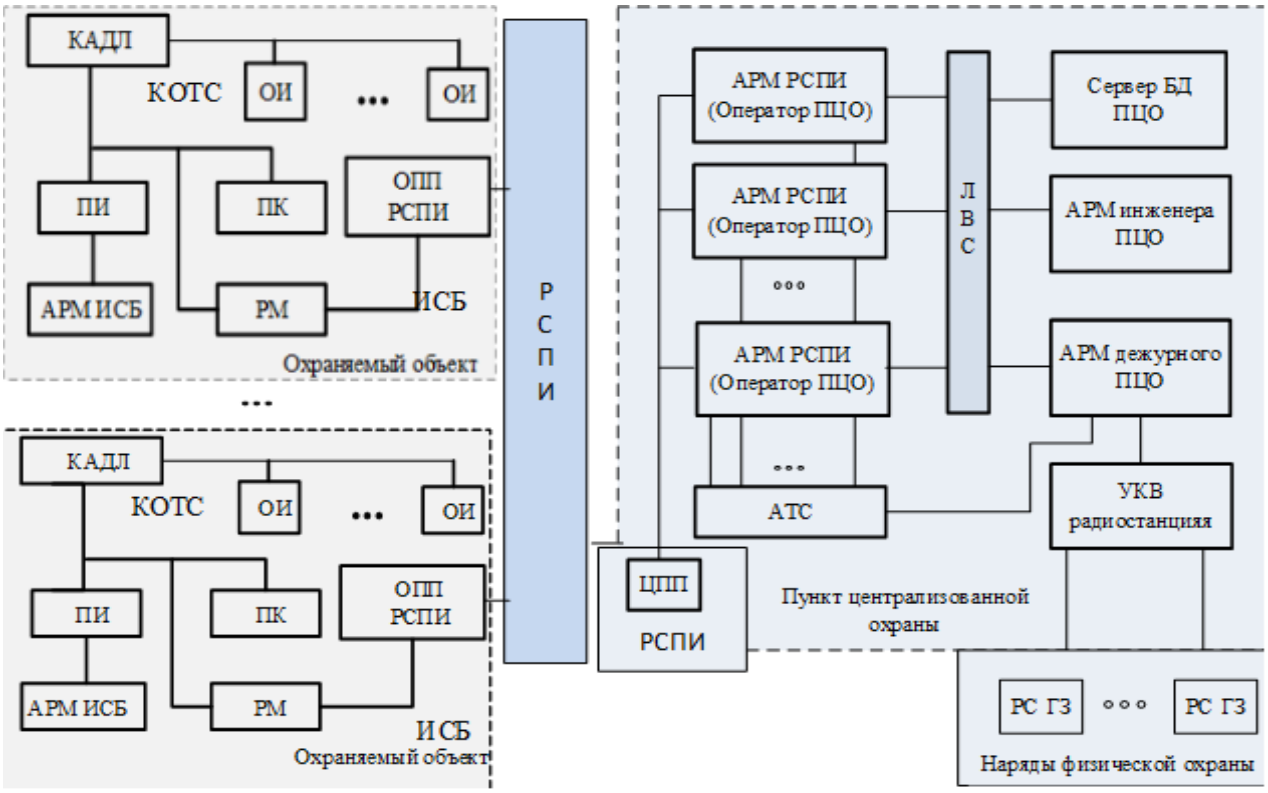
Структура и объем диссертационной работы. Диссертация состоит из введения, четырех глав, заключения, списка использованных источников из 114 наименований, 3 приложений и содержит 137 страниц основного текста, иллюстрированного 11 рисунками, содержит 21 таблицу.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность темы диссертации. Формулируются цель и задачи исследований.

В главе 1 анализируются особенности ТКС ЦОО (рис. 1), уточняются задачи исследования. Режимами функционирования (РФ) ТКС ЦОО будем называть определяемый в зависимости от обстановки порядок организации деятельности сил и средств, основные мероприятия, проводимые в деятельности.

Функциями ТКС ЦОО будем называть «сетевые сценарии», на базе которых обеспечивается работоспособность РФ. Принадлежности основных функций (ОФ) режимам задается функцией $\delta(a,b)=1$ $(a=1,\dots,A;\ b=1,\dots,B)$, если b-я ОФ «присутствует» в a-м режиме, иначе $\delta(a,b)=0$. Информационные процессы (ИП)ТКС - процессы создания, обработки, хранения и распространения информации. Принадлежности ИП ОФ задается функцией $\zeta(c,b)=1$ $(c=1,\dots,C)$, если c-й ИП «присутствует» в b-й ОФ, иначе $\zeta(a,b)=0$. Принадлежности компонентов ИП задается функцией $\eta(c,d)=1$ $(d=1,\dots,D)$, если d-й компонент «присутствует» в c-ом ИП, иначе $\eta(a,b)=0$.



КОС ОТС - комплекс объектовых средств охранно-тревожной сигнализации; КАДПЛ - контроллер адресной двухпроводной линии ОИ – объектовые извещатели охранно-тревожной сигнализации ($КОМ_1$); ПИ - преобразователь интерфейсов ПК – персональный компьютер ($КОМ_2$); РМ - релейные модули АРМ ИСБ – АРМ интегрированной системы безопасности ($КОМ_3$); ОПП - объектовый приёмо-передатчик ($КОМ_4$); РСПИ - система передачи извещений радиоканальная ($КОМ_5$); ПЦО - пункт централизованной охраны; ЦПП - центральный приемо-передатчик РСПИ ($КОМ_6$) ЛВС, АРМ РСПИ ($КОМ_7$); АТС – автоматическая телефонная станция ($КОМ_8$); АРМ дежурного ПЦО ($КОМ_9$) УКВ радиостанция ($КОМ_{10}$); РС ГЗ радиостанция группы задержания ($КОМ_{11}$)

Рис. 1 Структура ТКС ЦОО

Введем показатель работоспособности ТКС $ПР_{ТКС}=\{ПР_{ТКС}(ОР_1),\dots,ПР_{ТКС}(ОР_a),\dots,ПР_{ТКС}(ОР_A)\}$, здесь $ПР_{ТКС}(ОР_a)$ – ПР ТКС,

функционирующей в a-ом РФ; $\text{ПР}_{\text{ТКС}}\ (\text{ОР}_a) = \{\text{ПР}(\text{ОФ}_1^a),\ \ \dots\ ,\ \text{ПР}(\text{ОФ}_{B_a}^a)\}$, где $\text{ПР}(\text{ОФ}_b^a)$ - ПР b-й основной функции, обеспечивающей a-й РФ ($b = 1, \dots, B_a$); $\text{ПР}(\text{ОФ}_b^a) = \{\text{ПЗ}(\text{ИП}_1^{b,a}), \dots, \text{ПЗ}(\text{ИП}_{C_{b,a}}^{b,a})\}$, где $\text{ПЗ}(\text{ИП}_c^{b,a})$ - показатель защищенности c-го ИП, участвующего в обеспечении b-й ОФ a-го РФ ($c = 1, \dots, C_{b,a}$) - это минимальный показатель защищенности из всех $\text{ИП}_c^{b,a}$ («слабое звено»): $\text{ПР}(\text{ОФ}_b^a) = \min\limits_{C_{b,a}}\{\text{ПЗ}(\text{ИП}_1^{b,a}), \dots, \text{ПЗ}(\text{ИП}_{C_{b,a}}^{b,a})\}$; $\text{ПЗ}(\text{ИП}_c^{b,a}) = \{\text{ПЗ}(\text{КОМ}_1^{c,b,a}), \dots, \text{ПЗ}(\text{КОМ}_{D_{c,b,a}}^{c,b,a})\}$, где $\text{ПЗ}(\text{КОМ}_d^{c,b,a})$ - показатель защищенности d-го компонента ТКС, реализующего c-й ИП b-й функции a-го РФ ($d = 1, \dots, D_{c,b,a}$) - это минимальный показатель защищенности из всех $\text{КОМ}_d^{c,b,a}$ («слабое звено»): $\text{ПЗ}(\text{ИП}_c^{b,a}) = \min\limits_{D_{c,b,a}}\{\text{ПЗ}(\text{КОМ}_1^{c,b,a}), \dots, \text{ПЗ}(\text{КОМ}_{D_{c,b,a}}^{c,b,a})\}$.

В дальнейшем под показателем защищенности d-го компонента ТКС, участвующего в c-м ИП b-й ОФ a-го РФ будем понимать вероятность $p_d^{c,b,a}$ обеспечения требуемого уровня ИБ. Тогда $\text{ПЗ}(\text{ИП}_c^{b,a}) = \{p_1^{c,b,a}, \dots, p_{D_{c,b,a}}^{c,b,a}\}$.

Алгоритм определения вероятности защищенности компонента ТКС ЦОО (алгоритм 1)

Используется модель ИБ с полным перекрытием: множество угроз (УГ) d-му компоненту $\text{УГ}^d = \{\text{УГ}^d{}_1, \dots, \text{УГ}^d{}_g, \dots, \text{УГ}^d{}_{G_d}\}$; множество уязвимостей (У), выявленных в d-м компоненте $\text{У}^d = \{\text{У}^d{}_1, \dots, \text{У}^d{}_f, \dots, \text{У}^d{}_{F_d}\}$; множество защитных механизмов (ЗМ) d-го компонента $\text{ЗМ}^d = \{\text{ЗМ}^d{}_1, \dots, \text{ЗМ}^d{}_h, \dots, \text{ЗМ}^d{}_{H_d}\}$; матрица «угроза-уязвимость» $\|\lambda^d(g,f)\|$, $0 \le \lambda^d(g,f) \le 1$; матрица «угроза-защитный механизм» $\|\mu^d(g,h)\|$, $0 \le \mu^d(g,h) \le 1$.

Шаг 1. Рассчитаем вероятность того, что g-я угроза будет реализована хотя бы из-за одной из F_d уязвимостей $p^d(g,f) = 1 - \sum_{f=1}^{F_d}(1 - \hat{\lambda}^d(g,f)\ /F_d$.

Шаг 2. Рассчитаем вероятность «не прохождения» g-й угрозы через все ЗМ компонента $p^d(g,h) = 1 - \sum_{h=1}^{H_d}(1 - \hat{\mu}^d(g,h)\ )\ /H_d$.

Шаг 3. Рассчитаем показатель защищенности от k-й угрозы

$$p^d(g) = 1 - (p^d(g,f) \times\ (1 - p^d(g,h))).$$

Шаг 4. Найдем минимальный показатель защищенности $p^d = \min\limits_{G_d}\{p^d(1), \dots, p^d(G_d)\}$. Конец алгоритма.

Модель оценки работоспособности ТКС ЦОО

Шаг 1. $a = 1$. Начинаем с первого РФ.

Шаг 2. Сформировать множества: $\text{ОФ}^a = \{\text{ОФ}_1^a, \dots, \text{ОФ}_b^a, \dots, \text{ОФ}_{B_a}^a\}$, $\text{ИП}^{b,a} = \{\text{ИП}_1^{b,a}, \dots, \text{ИП}_c^{b,a}, \dots, \text{ИП}_{C_{b,a}}^{b,a}\}$ для всех ОФ_b^a $b = 1, \dots, B_a$, $\text{КОМ}^{c,b,a} = \{\text{КОМ}_1^{c,b,a}, \dots, \text{КОМ}_d^{c,b,a}, \dots, \text{КОМ}_{D_{c,b,a}}^{c,b,a}\}$, для всех $\text{ИП}_c^{b,a}$ $c = 1, \dots, C_{b,a}$.

Шаг 3. $b = 1$. С первой ОФ режима.

Шаг 4. $\text{c} = 1$. С первого ИП функции. $\text{ПР}(\text{ОФ}_b^a) = 1$.

Шаг 5. $d = 1$. С первого компонента ИП. $\text{ПЗ}(\text{ИП}_c^{b,a}) = 1$.

Шаг 6. Выполнить алгоритм 1; $p_d^{c,b,a} = p^d$; если $p_d^{c,b,a} < \text{ПЗ}(\text{ИП}_c^{b,a})$, то $\text{ПЗ}(\text{ИП}_c^{b,a}) = p_d^{c,b,a}$если $d < D_{c,b,a}$, то $d = d + 1$, перейти к шагу 6.

Шаг 7. Если $\text{ПЗ}(\text{ИП}_c^{b,a}) < \text{ПР}(\text{ОФ}_b^a)$ то $\text{ПР}(\text{ОФ}_b^a) = \text{ПЗ}(\text{ИП}_c^{b,a})$. Если $c < C_{b,a}$, то $c = c + 1$, перейти к шагу 5.

Шаг 8. $\text{ПР}_{\text{ТКС}}(\text{ОР}_a) = \{\text{ПР}(\text{ОФ}_1^a), \text{ПР}(\text{ОФ}_2^a), \dots, \text{ПР}(\text{ОФ}_{B_a}^a)\}$. Если $b < B_a$, то $b = b + 1$, перейти к шагу 4.

Шаг 9. Если $a \le A$, то $a = a + 1$, перейти к шагу 2. Иначе

$\text{ПР}_{\text{ТКС}} = \{\text{ПР}_{\text{ТКС}}(\text{ОР}_1), \dots, \text{ПР}_{\text{ТКС}}(\text{ОР}_a), \dots, \text{ПР}_{\text{ТКС}}(\text{ОР}_A)\}$, конец алгоритма.

Во второй главе на основании анализа результатов экспертного опроса 15 специалистов вневедомственной охраны Росгвардии России, нормативных источников государственных регуляторов и стандартов выявлено 16 уязвимостей, 12 защитных механизмов, 34 угрозы, 7 типов нарушителя и их взаимосвязи, характерных для ТКС ЦОО, что позволяет сроить модели угроз конкретной ТКС ЦОО.

Алгоритм оценки вероятности реализации угрозы при наличии уязвимости компонента ТКС ЦОО (Алгоритм 2)

Пусть для уязвимостей в *d*-м компоненте будет следующая систематизация $\text{У}^d(f, lf, mf, nf)$: f – номер; lf – индекс типа угроз, вызываемых уязвимостью (1 – вызывающая угрозу целостности (Ц); 2 – конфиденциальности (К); 3 – доступности (Д); 4 – Ц и К; 5 – Ц и Д; 6 – К и Д; 7 – Ц,К и Д); mf – индекс, определяющий способ выявления уязвимости (1 – проявляется в процессе экс-

плуатации; 2 – выявляется нормативно; 3 – выявляется объективно; 4 – определяется по расчетной методике; 5 – выявляется субъективно; 6 – выявляется субъективно оперативным путем; nf - индекс, определяющий характер проявления уязвимостей (1 – постоянная, 2 – периодическая редкая, 3 – периодическая частая; 4 – случайная).

Пусть для угроз для d-го компонента будет следующая систематизация $УГ^d(g, lg, ng)$: g – текущий номер; lg – индекс типа угроз (1 –угроза Ц; 2 – К; 3 – Д; 4 – Ц и К; 5 – Ц и Д; 6 – К и Д; 7 – Ц, К и Д); ng – индекс, определяющий характер проявления (1 – постоянная, 2 – периодическая редкая, 3 – периодическая частая; 4 – случайная).

Предлагается качественно определить влияние на $\lambda^d(g, f)$ каждой пары «Уязвимость – Угроза» как минимальное (min), максимальное (max) и среднее (сред) влияние. Введем:

- $\varphi^d(lf, mf, nf)$ – показатель «влияния» уязвимости на $\lambda^d(g, f)$, отдельно выделим $\varphi^d(lf)$ – показатель «влияния» типа угроз на $\lambda^d(g, f)$; $\varphi^d(mf)$ - показатель «влияния» способа выявления уязвимости на $\lambda^d(g, f)$; $\varphi^d(nf)$ - показатель «влияния» характера проявления уязвимостей на $\lambda^d(g, f)$;

- $\varphi^d(lg; ng)$ – показатель «влияния» угрозы на $\lambda^d(g, f)$, отдельно выделим $\varphi^d(lg)$ - показатель «влияния» типа угрозы на $\lambda^d(g, f)$; $\varphi^d(ng)$ - показатель «влияния» характера проявления угрозы на $\lambda^d(g, f)$.

Правило качественной оценки $\varphi^d(lf)$: если $lf = 7$ то $\varphi^d(lf) = "max"$, если $lf \in \{4; 5; 6\}$ то $\varphi^d(lf) =$ "сред", иначе $\varphi^d(lf) = \min(lf \in \{1; 2; 3\})$.

Правило качественной оценки $\varphi^d(mf)$: если $mf \in \{1; 2; 3\}$ то $\varphi^d(mf) = "max"$, если $mf = 4$ то $\varphi^d(mf) =$ "сред", наче $\varphi^d(mf) = \min(mf \in \{5; 6\})$.

Правило качественной оценки $\varphi^d(nf)$: если $nf \in \{1; 3\}$ то $\varphi^d(nf) = "max"$, если $nf = \{4\}$ то $\varphi^d(nf) =$ "сред", иначе $\varphi^d(nf) = "min"$ ($nf = 2$).

Правило качественной оценки $\varphi^d(lf, mf, nf)$: если $(\varphi^d(lf) = "max") \wedge (\varphi^d(mf) = "max") \wedge (\varphi^d(nf) = "max")$ то $\varphi^d(lf, mf, nf) = "max"$; если $(\varphi^d(lf) =$ «сред») $\wedge (\varphi^d(mf) = "max") \wedge (\varphi^d(nf) = "max")$ то $\varphi^d(lf, mf, nf) = "max"$; если $(\varphi^d(lf) = "min") \wedge (\varphi^d(mf) = "max") \wedge (\varphi^d(nf) = "max")$ то $\varphi^d(lf, mf, nf) =$ «сред»; если $(\varphi^d(lf) =$ "сред") $\wedge (\varphi^d(mf) =$ «сред» $\wedge (\varphi^d(nf) = "max")$ то $\varphi^d(lf, mf, nf) =$ «сред»; если $(\varphi^d(lf) = "min") \wedge (\varphi^d(mf) =$ "сред") $\wedge (\varphi^d(nf) = "max")$ то $\varphi^d(lf, mf, nf) =$ "сред"; если $(\varphi^d(lf) =$ "сред") $\wedge (\varphi^d(mf) =$ "сред") $\wedge (\varphi^d(nf) =$ "сред") то $\varphi^d(lf, mf, nf) =$

"сред"; если $(\varphi^d(lf) = "min") \wedge (\varphi^d(mf) = "min") \wedge (\varphi^d(nf) = "max")$ то $\varphi^d(lf, mf, nf)$ = "сред"; иначе $\varphi^d(lf, mf, nf) = "min"$.

Правило качественной оценки $\varphi^d(lg)$: если $lg = 7$ то $\varphi^d(lg) = "max"$, если $lg \in \{4; 5; 6\}$ то $\varphi^d(lg) =$ "сред", иначе $\varphi^d(lg) = "min"$.

Правило качественной оценки $\varphi^d(ng)$: если $ng \in \{1; 3\}$ то $\varphi^d(ng) = "max"$, если $ng = 4$ то $\varphi^d(ng) =$ "сред", иначе $\varphi^d(ng) = "min"$ $(ng = 2)$.

Правило качественной оценки $\varphi^d(lg; ng)$: если $(\varphi^d(lg) = "max") \wedge (\varphi^d(ng) = "max")$ то $\varphi^d(lg; ng) = "max"$; если $(\varphi^d(lg) = "min") \wedge (\varphi^d(ng) = "min")$ то $\varphi^d(lg; ng) = "min"$; иначе $\varphi^d(lg; ng) =$ "сред".

Рассмотрев все возможные варианты пар «Уязвимость – Угроза», эксперты выделили 10 устойчивых комбинаций, влияющих на возможность реализации угрозы как одно из списка: «Незначительное», «Низкое», «Ниже среднего», «Среднее», «Выше среднего», «Приемлемое», «Существенное», «Значительное», «Весьма значительное», «Катастрофическое».

С помощью логических конструкций был формализован данный подход. Переход от качественных значений к количественным (вероятностям) производится равномерно от 0,1 до 1,0 с шагом 0,1.

Количественная оценка $\hat{\lambda}^d(g, f)$: если ($\varphi^d(lf, mf, nf) = "max") \wedge (lf = 7) \wedge (\varphi^d(lg; ng) = "max")$ то $\hat{\lambda}^d(g, f) =$ «Катастрофическое» (1.0), если ($\varphi^d(lf, mf, nf) = "max") \wedge (lf \neq 7) \wedge (\varphi^d(lg; ng) = "max")$ то $\hat{\lambda}^d(g, f) =$ «Весьма значительное» (0.9), если ($\varphi^d(lf, mf, nf) = "max") \wedge (\varphi^d(lg; ng) =$ "сред") то $\hat{\lambda}^d(g, f) =$ «Значительное» (0.8), если ($\varphi^d(lf, mf, nf) =$ сред) $\wedge (\varphi^d(lg; ng) = "max")$ то $\hat{\lambda}^d(g, f) =$ «Существенное» (0.7), если ($\varphi^d(lf, mf, nf) = "max") \wedge (\varphi^d(lg; ng) = "min"$) то $\hat{\lambda}^d(g, f) =$ «Приемлемое» (0.6), если ($\varphi^d(lf, mf, nf) = "min") \wedge (\varphi^d(lg; ng) = "max")$ то $\hat{\lambda}^d(g, f) =$ «Выше среднего» (0.5), если ($\varphi^d(lf, mf, nf) =$ "сред") $\wedge (\varphi^d(lg; ng) =$ "сред") то $\hat{\lambda}^d(g, f) =$ «Среднее» (0.4), если ($\varphi^d(lf, mf, nf) =$ "сред") $\wedge (\varphi^d(lg; ng) = "min")$ то $\hat{\lambda}^d(g, f) =$ «Ниже среднего» (0.3), если ($\varphi^d(lf, mf, nf) = "min") \wedge (\varphi^d(lg; ng) =$ "сред") то $\hat{\lambda}^d(g, f) =$ «Низкое» (0.2), иначе $\hat{\lambda}^d(g, f) =$ «Незначительное» (0.1) (($\varphi^d(lf, mf, nf) = "min") \wedge (\varphi^d(lg; ng) = "min")$.

Алгоритм 2

Исходные данные: матрица связи угроз и уязвимостей

Шаг 1. $f = 1$. Начиная с первой угрозы.

Шаг 2 Начиная с первой уязвимости, связанной с текущей угрозой.

Шаг 3. Вычислить $\hat{\lambda}^d(g,f)$.

Шаг 4. Если есть еще уязвимости, связанные с угрозой с номером g, то перейти к следующей $f = f + 1$, перейти к шагу 3, иначе если не последняя угроза ($g \leq 34$), то $g = g + 1$ перейти к шагу 2 иначе конец алгоритма.

Алгоритм оценки вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов (Алгоритм 3)

Отличается от известных количественным способом оценки и вновь выявленными закономерностями между типами угроз, а также способом и характером действия защитных механизмов.

Пусть для ЗМ$^{\boldsymbol{d}}(h,p,k,nh)$ будет следующая систематизация: h –номер; p – тип ЗМ (1 – организационный; 2 – программный; 3 – технический; 4 – криптографический); k - индекс, определяющий тип действия ЗМ (1 – предотвращение Уг; 2 – недопущение Уг; 3 – повышения вероятности обнаружения Уг; 4 – снижение вероятности реализации Уг; 5 – предупреждение о реализации); nh - индекс, определяющий характер действия ЗМ (1 – постоянный, 2 – периодический редкий, 3 – периодический частый; 4 – случайный).

Предлагается качественно определить влияние на $\hat{\mu}^d(g,h)$ каждой пары «Защитный механизм – Угроза» как минимальное (min), максимальное (max) и среднее (сред) влияние. Для этого введем: $\varphi^d(p;k;nh)$ – показатель «влияния» типа h-го ЗМ и $\varphi^d(lg;ng)$ – показатель «влияния» типа g-й угрозы на $\hat{\mu}^d(g,h)$.

Правило количественной оценки $\hat{\mu}^d(g,h)$:

если $k = 5$ то $\varphi^d(p;k;nh) = "max"$, если $k = \{3;4\}$ то $\varphi^d(p;k;nh) =$ "сред", иначе $\varphi^d(p;k;nh) = "min"$ $(k \in \{1;2\})$; если $nh = 2$ то $\varphi^d(p;k;nh) = "max"$, если $nh = 4$ то $\varphi^d(p;k;nh) =$ "сред", иначе $\varphi^d(p;k;nh) = "min"$) $nh \in \{1;3\}$);

если $(\varphi^d(p;k;nh) = "max") \wedge (k = 5) \wedge (\varphi^d(lg;ng) = "max")$ то $\hat{\mu}^d(g,h) =$ "Катастрофическое" (1.0) , если $(\varphi^d(p;k;nh) = "max") \wedge (k \neq 5) \wedge (\varphi^d(lg;ng) = "max")$ то $\hat{\mu}^d(g,h) = 0.9$, если $(\varphi^d(p;k;nh) = "max") \wedge (\varphi^d(lg;ng) =$ "сред") то $\hat{\mu}^d(g,h) = 0{,}8$, если $(\varphi^d(p;k;nh) =$ "сред") $\wedge (\varphi^d(lg;ng) = "max")$ то $\hat{\mu}^d(g,h) = 0{,}7$, если $(\varphi^d(p;k;nh) = "max") \wedge (\varphi^d(lg;ng) = "min")$ то $\hat{\mu}^d(g,h = 0{,}6$, если $(\varphi^d(p;k;nh) = "min") \wedge (\varphi^d(lg;ng) = "max")$ то $\hat{\mu}^d(g,h) = 0{,}5$, если $(\varphi^d(p;k;nh) =$

"сред") ∧ ($\varphi^d(lg; ng)$ = "сред") то $\hat{\mu}^d(g,h) = 0{,}4$, если ($\varphi^d(p; k; nh)$ = "сред") ∧ ($\varphi^d(lg; ng)$ = "min") то $\hat{\mu}^d(g,h) = 0{,}3$, если ($\varphi^d(p; k; nh)$ = "min") ∧ ($\varphi^d(lg; ng)$ = "сред") то $\hat{\mu}^d(g,h) = 0{,}2$, иначе $\hat{\mu}^d(g,h) = 0{,}1$ (($\varphi^d(p; k; nh)$ = "min")∧($\varphi^d(lg; ng)$ = "min").

Алгоритм 3

Исходные данные: матрица связи угроз и защитных механизмов

Шаг 1. $f = 1$. Начиная с первой угрозы.

Шаг 2 Начиная с первого ЗМ, связанного с текущей угрозой.

Шаг 3. Вычислить $\hat{\mu}^d(g,h)$.

Шаг 4. Если есть еще защитные механизмы, связанные с угрозой с номером g, то перейти к следующему ЗМ $h = h + 1$, перейти к шагу 3, иначе если не последняя угроза ($g \leq 34$), то $g = g + 1$ перейти к шагу 2 иначе конец алгоритма.

Усовершенствованная модель определения вероятности защищенности компонента ТКС ЦОО от угроз

Оригинальность модели состоит в том, что включен элемент «Нарушитель» и сопутствующие ему параметры.

Модель нарушителя Н(q, s): q - индекс, определяющий тип нарушителя по возможности доступа к ТКС (1 – внутренний, осведомлен об оперативной информации; 2 – внутренний, может модифицировать информацию; 3 – внутренний, имеет доступ к ТКС и принимает решения по реагированию; 4 – внешний, не обладает информацией об объекте и доступом к ТКС; 5 – внешний, обладает информацией об объекте, но не имеющий доступа к ТКС; 6 – внешний, обладающий информацией об объекте, может быть осведомлен об оперативной информации в ТКС; 7 – внешний, обладает информацией об объекте, имеет доступ и способен модифицировать или саботировать информацию в ТКС); s - индекс, определяющий оснащенность нарушителя (1 – неоснащенный; 2 – частично оснащенный; 3 – полностью оснащенный, имеющий любые технические и программные средства).

Дополнительно введем параметр $NP(g, \text{Н})$, учитывающий возможности нарушителя реализовать угрозу ($NP(q,s) \in [0,1]$). Предлагается качественно определить влияние на $NP(g, \text{Н})$ каждой пары «Нарушитель – Угроза» как "min", "max" и "сред" влияние. Для этого введем показатели «влияния» на

$NP(g, \text{Н})$ типа нарушителя $\varphi^d(q,s)$ и типа угрозы $\varphi^d(lg;ng)$. Введем параметр $YP(g,t)$ - вероятность посягательства с целью реализации угроз $YP(g,t) \in [0,1]$, здесь t - индекс, определяющий категорию охраняемого объекта (1 – А1; 2 – А2; 3 – А3; 4 – Б1; 5 – Б2).

Предлагается качественно определить влияние на $\widehat{YP}(g,t)$ каждой пары «Категория охраняемого объекта / Угроза» "min", "max" и "сред" влияние. Введем показатели «влияния» на $\widehat{YP}(g,t)$: категории охраняемого объекта $\varphi^d(t)$, типа g-й угрозы $\varphi^d(lg;ng)$.

Правило количественной оценки $\widehat{NP}(g, \text{Н})$:

если $q \in \{1;2;3;7\}$ то $\varphi^d(q,s) = "max"$, если $q \in \{5;6\}$ то $\varphi^d(q,s) NP(g, \text{Н}) = "\text{сред}"$, иначе $\varphi^d(q,s) = "min"$ $(q = 4)$; если $s = 3$ то $\varphi^d(q,s) = "max"$, если $s = 2$ то $\varphi^d(q,s) = "\text{сред}"$, иначе $\varphi^d(q,s) = \min$ $(s = 1)$; Если $(\varphi^d(q,s) = "max") \wedge (q = 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g, \text{Н}) = 1$, если $(\varphi^d(q,s) = "max") \wedge (q \neq 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g, \text{Н}) = 0.9$, если $(\varphi^d(q,s) = "max") \wedge (\varphi^d(lg;ng) = "\text{сред}")$ то $\widehat{NP}(g, \text{Н}) = 0{,}8$, если $(\varphi^d(q,s) = "\text{сред}") \wedge (\varphi^d(lg;ng)$ "max") то $\widehat{NP}(g, \text{Н}) = 0{,}7$, если $(\varphi^d(q,s) = "max") \wedge (\varphi^d(lg;ng) = "min")$ то $\widehat{NP}(g, \text{Н}) = 0{,}6$, если $(\varphi^d(q,s) = "min") \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g, \text{Н}) = 0{,}5$, если $(\varphi^d(q,s) = "\text{сред}") \wedge (\varphi^d(lg;ng) = "\text{сред}")$ то $\widehat{NP}(g, \text{Н}) = 0{,}4$, если $(\varphi^d(q,s) = "\text{сред}") \wedge (\varphi^d(lg;ng) = "min")$ то $\widehat{NP}(g, \text{Н}) = 0{,}3$, если $(\varphi^d(q,s) = "min") \wedge (\varphi^d(lg;ng) = "\text{сред}")$ $\widehat{NP}(g, \text{Н}) = 0{,}2$, иначе $\widehat{NP}(g, \text{Н}) = 0{,}1$ $(\varphi^d(q,s) = "min") \wedge (\varphi^d(lg;ng) = "min")$.

Правило количественной оценки $\widehat{YP}(g,t)$:

если $q \in \{1;2;3;7\}$ то $\varphi^d(q,s) = "max"$, если q $\{5;6\}$ то $\varphi^d(q,s) NP(g, \text{Н}) = "\text{сред}"$, иначе $\varphi^d(q,s) = "min"$ $(q = 4)$; если $s = 3$ то $\varphi^d(q,s) = \max$, если $s = 2$ то $\varphi^d(q,s) = "\text{сред}"$, иначе $\varphi^d(q,s) = \min$ $(s = 1)$; Если$(\varphi^d(q,s) = "max") \wedge (q = 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g, \text{Н}) = 1$, если $(\varphi^d(q,s) = "max") \wedge (q \neq 1) \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g, \text{Н}) = 0.9$, если $(\varphi^d(q,s) = "max") \wedge (\varphi^d(lg;ng) = "\text{сред}")$ то $\widehat{NP}(g, \text{Н}) = 0{,}8$, если $(\varphi^d(q,s) = "\text{сред}") \wedge (\varphi^d(lg;ng) = "max"$, то $\widehat{NP}(g, \text{Н}) = 0{,}7$, если $(\varphi^d(q,s) = "max") \wedge (\varphi^d(lg;ng) = "min")$ то $\widehat{NP}(g, \text{Н}) = 0{,}6$, если $(\varphi^d(q,s) = "min") \wedge (\varphi^d(lg;ng) = "max")$ то $\widehat{NP}(g, \text{Н}) = 0{,}5$, если $(\varphi^d(q,s) = "\text{сред}") \wedge (\varphi^d(lg;ng) = "\text{сред}")$ то $\widehat{NP}(g, \text{Н}) = 0{,}4$, если $(\varphi^d(q,s) = "\text{сред}") \wedge (\varphi^d(lg;ng) = "min")$ то $\widehat{NP}(g, \text{Н}) = 0{,}3$, если $(\varphi^d(q,s) = "min") \wedge (\varphi^d(lg;ng) = "\text{сред}")$ $\widehat{NP}(g, \text{Н}) =$

0,2, иначе $\widehat{NP}(g,\text{Н}) = 0{,}1$ $((\varphi^d(q,s) = \text{"}min\text{"}) \wedge (\varphi^d(lg;ng) = \text{"}min\text{"})$.

Вероятность реализации g-й угрозы из-за f -й уязвимости для d-го структурного компонента ТКС ЦОО $p^d(g,f) = 1 - \sum_{f=1}^{F_d}(1 - \hat{\lambda}^d(g,f))\,/F_d$. Вероятность опасности угроз по последствиям их реализации с учетом ЗМ - «степень сопротивляемости» g - й угрозе h –го ЗМ для d-го структурного компонента ТКС ЦОО $p^d(g,h) = 1 - \sum_{h=1}^{H_d}(1 - \hat{\mu}^d(g,h))\,/H_d$. Показатель защищенности структурного компонента d ТКС от g-й угрозы, исходящей от нарушителя типа $\text{Н}(q,s)$ для охраняемого объекта категории t $p^d(g)|_{\text{Н}(q,s)} = 1 - [p^d(g,f) \times (1 - p^d(g,h)) \times \widehat{YP}(g,t) \times \widehat{NP}(g,\text{Н})]$.

Пусть на ПЦО охраняется объектов разных категорий $N|_t$. Тогда $p^d(g)|_{\text{Н}(q,s)} = \min\limits_{t=1,\dots,5}\left(\frac{\sum_{n=1}^{N|_t}(p^d(g)|_{\text{Н}(q,s)})}{N|_t}\right)$.

В 3 главе разрабатываются алгоритмы определения степени проявления уязвимости и силы защитных механизмов в компонентах ТКС ЦОО.

Для d-го компонента пронумерованное множество уязвимостей представим в виде: $\text{У}^d = \{\text{У}^d{}_1, \dots, \text{У}^d{}_f, \dots, \text{У}^d_{F_d}\}$, где $F_d \in F$. Далее рассматриваем уязвимости одного компонента ТКС ЦОО. Считаем, что f-я уязвимость может быть однозначно идентифицирована в компоненте по $r_{f_d} \in R$ признакам, R - множество всех возможных идентификационных признаков: $R = r_{\text{У}_1}, \dots, r_{\text{У}_f}, \dots, , r_{\text{У}_f}$ - подмножество идентификационных признаков f-й уязвимости компонента.

Идентификационным признаком уязвимости назовем такое событие в компоненте ТКС, которое определяет вид уязвимости. Предполагаем, что одна и та же уязвимость, находясь в разных компонентах, может проявляться более или менее. Такой качественной оценке сопоставим количественный эквивалент $s_{\text{У}_f} \in [0,1]$, где $s_{\text{У}_f}$ - степень проявления f-й уязвимости. $s_{\text{У}_f}$ показывает, какая часть f-й уязвимости присутствует (проявляется) в данном компоненте.

Введем множество $r^*{}_{\text{У}_f u_f}$ качественных параметров, характеризующих степень проявления u_f-го идентификационного признака f-й уязвимости: $r^*{}_{\text{У}_f u_f} = r^*{}_{\text{У}_f u_f 1}, \dots, r^*{}_{\text{У}_f u_f q(u_f)}, \dots, r^*{}_{\text{У}_f u_f Q(u_f)}$.

Алгоритм проявления уязвимостей *d*-го компонента (Алгоритм 4)

Исходные данные: множество $У^d$; для каждой $У^d{}_f$ имеются $r_{f_d} \in R$ признаков; $s_{У_{f\,ПОР}}$ (минимально возможное проявление).

Шаг 1. $f = 1$. Начинаем с первой уязвимости.

Шаг 2. Пронумеруем элементы подмножества идентификационных признаков f-й уязвимости компонента $r_{У_f} = r_{У_f 1}, \dots, r_{У_f u_f}, \dots, r_{У_f U_f}$.

Шаг 3. Введем категорию – «вес» (важность) признака $\tilde{r}_{У_f u_f} \in [0,1]$, (определен экспертами, $\sum_{u_f=1}^{U_f} \tilde{r}_{У_f u_f} = 1$).

Шаг 4. Введем множество $r^*{}_{У_f u_f}$ взаимоисключающих качественных параметров $r^*{}_{У_f u_f} = r^*{}_{У_f u_f 1}, \dots, r^*{}_{У_f u_f q(u_f)}, \dots, r^*{}_{У_f u_f Q(u_f)}$, качественной оценке сопоставим количественный эквивалент - $\widetilde{r^*}_{У_f u_f q(u_f)} \in [0,1]$, $\widetilde{r^*}_{У_f u_f q(u_f)}$ определяется экспертами по вкладу элемента в значение признака.

Шаг 5. Степень проявления f-й уязвимости определим по формуле $s_{У_f} = \sum_{u_f=1}^{U_f} \tilde{r}_{У_f u_f} \widetilde{r^*}_{У_f u_f q(u_f)}$.

Шаг 6. Если $s_{У_f} < s_{У_{f\,ПОР}}$ то $s_{У_f} = 0$ (уязвимость отсутствует). Если $f = F_d$ то конец алгоритма, иначе $f = f + 1$, перейти к шагу 2.

Отдельные результаты расчета весов идентификационных признаков уязвимостей и степеней их проявления сведены в табл. 1.

Таблица 1

$r_{У_f}$ $\tilde{r}_{У_f u_f}$	$r^*{}_{У_f u_f}$	$\widetilde{r^*}_{У_f u_f q(u_f)}$
$У_1$ - Нарушение условий эксплуатации ТСО		
$r_{У_{1}1}$ - Климатические условия не соответствуют РД $\tilde{r}_{У_{1}1}$ =0,32	$r^*{}_{У_{1}11}$ - Критические нарушения (отличаются более 50% от нормы), приводят выходу из строя ТСО	$\widetilde{r^*}_{У_{1}11} = 1$
	…	
	$r^*{}_{У_{1}14}$ - Допустимые отклонения (до 10% от нормы), приводят к сокращению срока службы ТСО	$\widetilde{r^*}_{У_{1}14} = 0.3$
$r_{У_{1}2}$ - Свободный доступ к щитам ОТС и оборудованию ТСО $\tilde{r}_{У_{1}2}$ =0,28	$r^*{}_{У_{1}21}$ - Свободный доступ любых сотрудников объекта	$\widetilde{r^*}\lambda_{У_{1}21}$ =0.7
	$r^*{}_{У_{1}22}$ - Свободный доступ любых сотрудников объекта и посетителей	$\widetilde{r^*}_{У_{1}22} = 1$
	…	
$r_{У_{1}4}$ - Форс-мажорные ситуации, приводящие к отказу ТСО $\tilde{r}_{У_{1}4}$= 0,11	$r^*{}_{У_{1}41}$ - Весьма вероятно для данного компонента	$\widetilde{r^*}_{У_{1}41} = 0.9$
	$r^*{}_{У_{1}42}$ - Мало вероятно для данного компонента	$\widetilde{r^*}_{У_{1}42} = 0.5$
	$r^*{}_{У_{1}43}$ - Почти невероятно для данного компонента	$\widetilde{r^*}_{У_{1}43} = 0.2$

Под способами защиты (далее защитными механизмами (ЗМ) обеспечения ИБ) понимаются организованные возможности средств и мероприятий, осуществляемых в ТКС ЦОО с целью полной или частичной реализации одного или нескольких методов (стратегий, функций) защиты. Множество ЗМ представим в виде объединения подмножеств ЗМ, «присущих» компонентам ТКС $\text{ЗМ} = \text{ЗМ}^1 \cup \text{ЗМ}^2 \cup \ldots \cup \text{ЗМ}^d \cup \ldots \cup \text{ЗМ}^D$. В дальнейшем для простоты будем считать, что конкретные ЗМ «закрепляются» за «своими» компонентами. Так для d-го компонента пронумерованное множество ЗМ представим в виде: $\text{ЗМ}^d = \{\text{ЗМ}^d{}_1, \ldots, \text{ЗМ}^d{}_h, \ldots, \text{ЗМ}^d_{H_d}\}$, где $H_d \in H$.

Далее рассматриваем ЗМ одного (d-го) компонента ТКС ЦОО. Предполагаем, что один и тот же ЗМ, находясь в разных компонентах и в разных условиях функционирования, может защищать компонент с разной «силой». Такой качественной оценке сопоставим количественный эквивалент $w_{\text{ЗМ}_h} \in [0,1]$ - силу (степень проявления) h-го ЗМ. $w_{\text{ЗМ}_h}$ показывает, какая часть максимально возможной силы h-го защитного механизма, характеризующейся множеством технических средств и организационно-технических мероприятий ($\text{СР}_{\text{ЗМ}_h} = \{\text{СР}_{\text{ЗМ}_h 1}, \ldots, \text{СР}_{\text{ЗМ}_h z_h}, \ldots, \text{СР}_{\text{ЗМ}_h Z_h}\}$) реально защищает компонент. Фрагмент перечня ЗМ и соответствующих им технических средств и организационно-технических мероприятий приведен в табл. 2.

Таблица 2

Наименование	Обозначение и наименование СР
Обеспечение требований по условиям эксплуатации ТСО ЗМ_1	$\text{СР}_{\text{ЗМ}_1 1}$ – Выполнение требований по климатическим условиям эксплуатации
	…
	$\text{СР}_{\text{ЗМ}_1 3}$ – Своевременное и качественное обследование охраняемых объектов
…	
Обеспечение требований эксплуатации РСПИ ЗМ_4	$\text{СР}_{\text{ЗМ}_4 1}$ – Не допущение действия дестабилизирующих факторов на объектовые и пультовые блоки РСПИ
	….
	$\text{СР}_{\text{ЗМ}_4 3}$ – Правильный монтаж антенн объектовых блоков РСПИ, контроль программирования объектовых блоков РСПИ

Введем дополнительные параметры: наличия/отсутствия h-го ЗМ - $\zeta(\text{ЗМ}_h, z_h) = 1$, если $\text{СР}_{\text{ЗМ}_h z_h}$ «выявлен» при анализе ЗМ_h, иначе $\zeta(\text{ЗМ}_h, z_h) = 0$; вес $\text{СР}_{\text{ЗМ}_h z_h}$ в h-м ЗМ - $\widetilde{w}(\text{ЗМ}_h, z_h) \in [0,1]$, $\sum_{,z_h=1}^{Z_h} \widetilde{w}(\text{ЗМ}_h, z_h) = 1$. Значение $\widetilde{w}(\text{ЗМ}_h, z_h)$ определяется экспертами. При данном подходе $w_{\text{ЗМ}_h} = \sum_{z_h=1}^{Z_h} \widetilde{w}(\text{ЗМ}_h, z_h) * \zeta(\text{ЗМ}_h, z_h)$.

Алгоритм определения силы защитных механизмов (Алгоритм 5)

Исходные данные: множество ЗМ; множество $\mathrm{СР}_{\mathrm{ЗМ}_h}$ технических средств и мероприятий определяющих ${\mathrm{ЗМ}^d}_h$; вес (показатель важности, определяется экспертами) $\mathrm{СР}_{\mathrm{ЗМ}_h z_h}$ в h-м защитном механизме $\widetilde{w}(\mathrm{ЗМ}_h, z_h) \in [0,1]$, $\sum_{,z_h=1}^{Z_h} \widetilde{w}(\mathrm{ЗМ}_h, z_h) = 1$; $w_{\mathrm{ЗМ}_h \mathrm{ПОР}}$ (минимальная сила).

Шаг 1. Пронумеруем элементы множества ЗМ для d-го компонента: $\mathrm{ЗМ}^d = \{{\mathrm{ЗМ}^d}_1, \dots, {\mathrm{ЗМ}^d}_h, \dots, \mathrm{ЗМ}^d_{H_d}\}$, где $H_d \in H$.

Шаг 2. $h = 1$ (с первого защитного механизма).

Шаг 3. Определить и запомнить все $\zeta(\mathrm{ЗМ}_h, z_h)$ - параметр наличия / отсутствия элемента $\mathrm{СР}_{\mathrm{ЗМ}_h z_h}$ в $\mathrm{ЗМ}_h$ - $\zeta(\mathrm{ЗМ}_h, z_h) = 1$, если $\mathrm{СР}_{\mathrm{ЗМ}_h z_h}$ «выявлен» при анализе $\mathrm{ЗМ}_h$, иначе $\zeta(\mathrm{ЗМ}_h, z_h) = 0$.

Шаг 4. Силу защитного механизма определим по формуле $w_{\mathrm{ЗМ}_h} = \sum_{z_h=1}^{Z_h} \widetilde{w}(\mathrm{ЗМ}_h, z_h) * \zeta(\mathrm{ЗМ}_h, z_h)$.

Шаг 5. Если $w_{\mathrm{ЗМ}_h} < w_{\mathrm{ЗМ}_h \mathrm{ПОР}}$ то $w_{\mathrm{ЗМ}_h} = 0$ (нет ЗМ). Если $h = H_d$ то конец алгоритма, иначе $h = h + 1$, перейти к шагу 3.

В **главе 4** разрабатываются средства автоматизации оценки работоспособности ТКС ЦОО, анализируются результаты расчетов работоспособности для конкретного мини-ПЦО. Обобщенный алгоритм автоматизированной оценки работоспособности ТКС на основе анализа защищенности информационных процессов приведен на рис.2.

Проведен пробный пример расчетов работоспособности ТКС ЦОО для конкретного мини-ПЦО. С этой целью были собраны и обезличены данные по результатам обследования о 25 объектах разных категорий. В результате были получены расчеты защищенности структурных элементов и информационных процессов ТКС ЦОО для объектов разных категорий и двух типов нарушителей (рис. 3).

По результатам расчётов выявлено, что защищенность объектов для всех категорий превышает 80%, что соответствует фактическому состоянию охраны по экспертным оценкам, наиболее слабым структурным элементом является связь дежурного ПЦО с нарядами охраны. При снижении категории объекта,

его уровень защищенности падает, что объясняется ростом недостатков в организации охраны, увеличением уязвимостей и снижении количества и качества функционирования защитных механизмов. При повышении возможностей нарушителя (повышении опасности нарушителя), защищенность объектов всех категорий снижается.

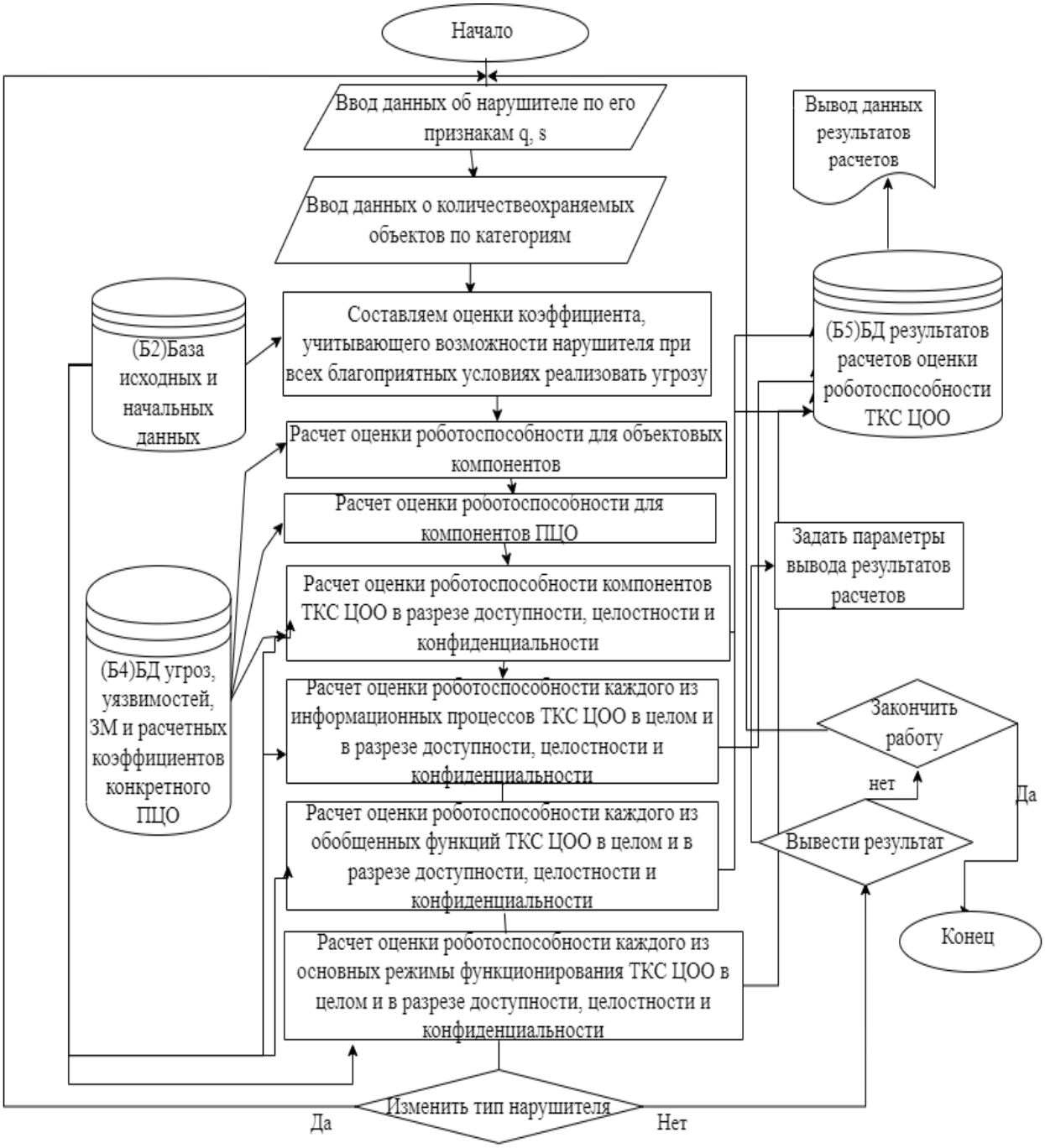


Рис. 2 Обобщенный алгоритм автоматизированной оценки работоспособности ТКС ЦОО

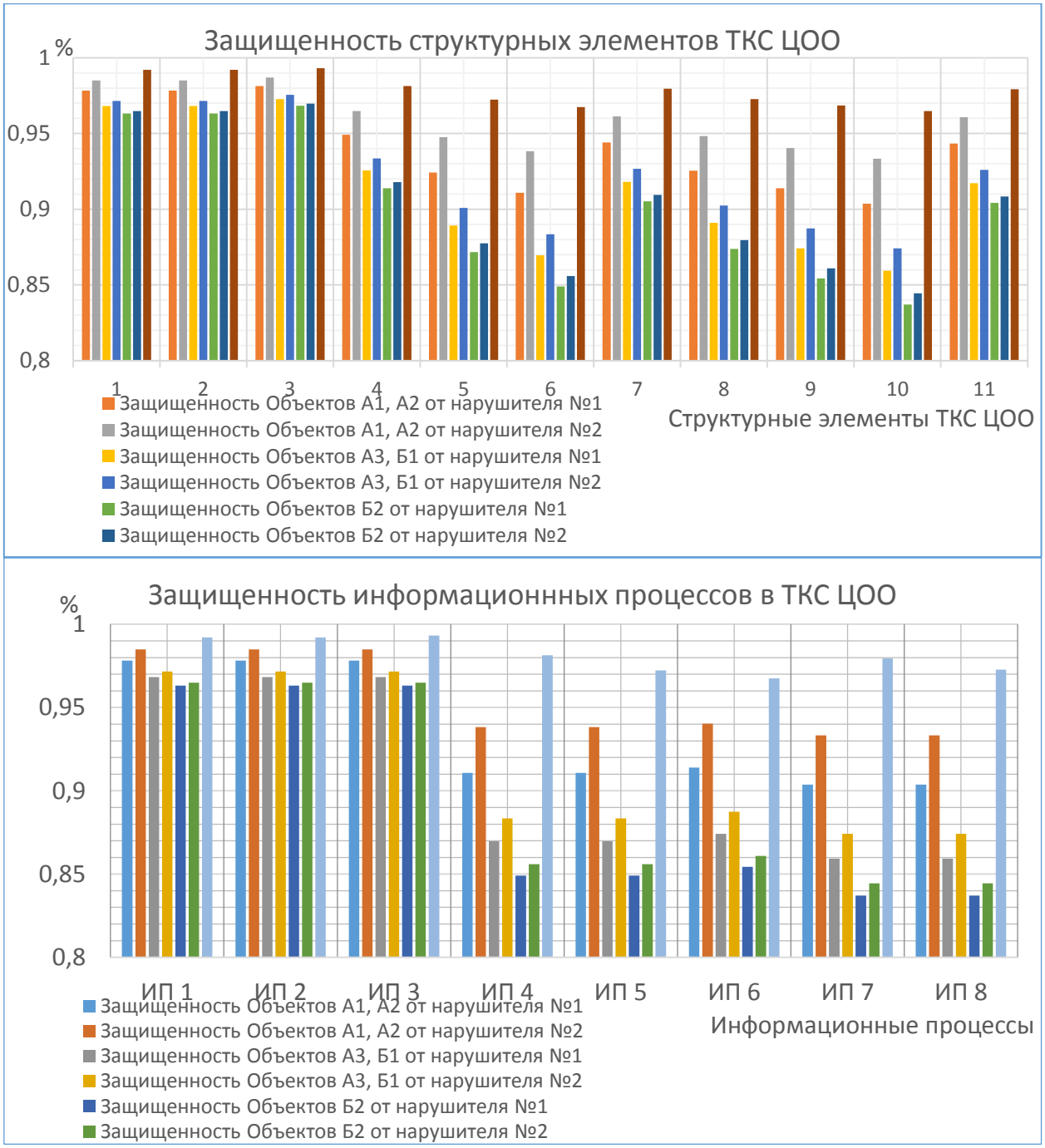


Рис. 3 Результаты расчета защищенности ТКС ЦОО

Основные результаты

Предложена формальная модель показателя работоспособности как функции вероятностей защищенности компонентов ТКС от множества угроз.

Синтезированы базы данных уязвимостей, угроз, защитных механизмов, типов нарушителя и их взаимосвязи, отличающиеся универсальностью и разумной достаточностью для систем данного типа.

Разработаны алгоритмы: (1) оценки вероятности реализации угрозы при

наличии уязвимости компонента ТКС ЦОО, отличающийся вновь выявленными закономерностями между типом угроз и способами проявления уязвимостей; (2) оценки вероятности опасности угроз в компонентах ТКС ЦОО с учетом защитных механизмов, отличающийся вновь выявленными закономерностями между типом угроз, способом и характером действия защитных механизмов; (3) определения степени проявления уязвимостей и (4) силы защитных механизмов, выявляемых в компонентах ТКС ЦОО, оригинальность которого основана на их декомпозиции в зависимости от условий эксплуатации компонентов.

Усовершенствована модель оценки вероятности информационной защищенности компонента ТКС ЦОО, оригинальность которой состоит в том, что в модель включен элемент «Нарушитель» и сопутствующие ему параметры.

Разработан обобщенный алгоритм автоматизированной оценки работоспособности ТКС ЦОО. При автоматизации расчетов предлагается ведение баз данных структурных компонентов, информационных процессов, обобщенных функций, основных режимов, матриц связности уязвимостей, угроз, ЗМ и структурных компонентов, распределения угроз по доступности, целостности и конфиденциальности, правил оценки вероятности эксплуатации угрозой уязвимости, опасности угроз, возможностей нарушителя.

Проведены расчеты работоспособности ТКС ЦОО для мини-ПЦО. Собраны данные по результатам обследования о 25 объектах разных категорий. В результате были получены оценки защищенности структурных компонентов и информационных процессов для объектов разных категорий и типов нарушителей. Выявлено, что самым низко защищенным компонентом являются объектовые комплексы ТСО.

Расчеты работоспособности структурных компонентов ТКС мини-ПЦО показывают, что уровень ошибок 2 рода (допущение НСД на защищаемый объект) отличается у них примерно на 8-10%. При этом основное отличие у объектов разных категорий состоит в снижении эффективности действия ЗМ объектовых комплексов ТСО при снижении категории объектов. В целом результаты расчетов соответствуют сложившейся практике функционирования ТКС ЦОО.

Научное развитие исследования автор связывает с дальнейшей автоматизацией процессов оценки работоспособности ТКС ЦОО, что позволит оперативно прогнозировать изменение состояния работоспособности всех структурных компонентов ТКС ЦОО при приеме под охрану новых объектов.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ТЕМЕ ДИССЕРТАЦИИ

Научные статьи, опубликованные в журналах из перечня ВАК

1. Тельный А.В., Черников Р.С. Алгоритм обработки тревожных извещений объектовых средств охранной сигнализации для снижения уровня ложных срабатываний // Системы управления, связи и безопасности. – 2019. – № 4. – С. 140-162.

2. Тельный, А. В., Черников Р. С., Яковлева Е. И. О возможности локализации местоположения устройства съема информации по радиоканалу // Проектирование и технология электронных средств. – 2020 – № 2. – С. 16-22.

Публикации в прочих изданиях

3. Черников, Р. С., Путренкова, К. А. Актуальные проблемы обеспечения информационной безопасности объектов уголовно-исполнительной системы // Вестник ФКУ НИИИТ ФСИН России: научно-практическое издание. – Тверь, 2019. – С. 140-143.

4. Монахов, М.Ю., Тельный, А.В., Черников, Р.С., Вилкова В.А. Логико-вероятностный подход в оценке безопасности телекоммуникационной системы централизованной охраны объектов // в сборнике ПТСПИ-2021 Материалы XIV международной научно-технической конференции. г. Владимир. – 2021. – С. 218-222.

5. Черников, Р. С. Некоторые аспекты применения биометрической идентификации в учреждениях и органах уголовно-исполнительной системы // Информационные технологии в УИС. – 2020. – № 3. –С. 53-58.

6. Тельный, А. В., Черников, Р. С., Шаров, В. А. О возможности использования ситуационной видеоаналитики // Шуйская сессия студентов, аспирантов, педагогов, молодых ученых: Материалы XIII Международной научной конференции, Москва-Иваново-Шуя, 2020. – С. 224-227.

7. Шаров, В. А., Черников Р. С., Тельный, А. В. О типовом методологическом подходе анализа показателей состояния информационной безопасности на основе использования экспертных оценок // Материалы XIII Международной научной конференции, Москва-Иваново-Шуя, 2020. – С. 230-233.

8. Черников, Р. С. Особенности методики применения нелинейных локаторов при проведении мероприятий по обнаружению технических средств и устройств // V Международный пенитенциарный форум "Преступление, наказание, исправление": Сборник тезисов. – Рязань: Академия права и управления ФСИН, 2021. – С. 307-311.

9. Тельный, А. В., Вилкова, В. А., Черников, Р. С. Об эффективности использования технических средств контроля несения службы нарядами физической охраны // FISP-2021: Фундаментальные проблемы информационной безопасности в условиях цифровой трансформации: Сборник докладов III Всероссийской научной конференции (с приглашением зарубежных ученых), Ставрополь, 2021. – С. 100-105.

10. Монахов, М. Ю., Тельный, А. В., Черников, Р. С., Вилкова, В. А. Использование рекуррентных методов в прогнозировании состояния защищенности информационных ресурсов телекоммуникационной сети // в сборнике ПТСПИ-2021 Материалы 14-ой международной научно-технической конференции, Владимир, 2021. – С. 218-222.

11. Черников, Р. С. Особенности методики применения сканерных приемников и программно-аппаратных комплексов радиоконтроля // Актуальные вопросы информатизации: Сборник материалов IV круглого стола. – ФКУ НИИИТ ФСИН России Тверь: 2022. – С. 276-282.

12. Черников Р.С. Программа оценки вероятности опасности угроз по последствиям их реализации с учетом защитных механизмов [Текст]: свидетельство о регистрации программы для ЭВМ №2022682661 / Матвеева Е.А., Вилкова В.А., Тельный А.В., Монахов М.Ю. - №2022682661; заявл. 20.10.2022; зарегистр. 24.11.2022.

13. Черников Р.С. Программа оценки вероятности эксплуатации угрозой уязвимости компонента ТКС ЦОО [Текст]: свидетельство о регистрации программы для ЭВМ №2022680341 / Матвеева Е.А., Вилкова В.А., Тельный А.В., Монахов М.Ю. - №2022680341; заявл. 20.10.2022; зарегистр. 31.10.2022.

Черников Роман Сергеевич

МОДЕЛИ И АЛГОРИТМЫ ОЦЕНКИ РАБОТОСПОСОБНОСТИ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ЦЕНТРАЛИЗОВАННОЙ ОХРАНЫ ОБЪЕКТОВ

Автореферат

диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 04.07.2023 г.
Формат 60×84/16. Усл. печ. л. 1,0. Тираж 100 экз.
Издательство Владимирского государственного университета
имени Александра Григорьевича и Николая Григорьевича Столетовых
600000, Владимир, ул. Горького, 87.