МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(Дипломная работа)

На тему « Создание модели безопасности информации образовательной организации **»**

Исполнитель _____ Нероев Егор Максимович

(подпись) (фамилия, имя, отчество)

Руководитель _____ Козлов Юрий Викторович

(подпись) (фамилия, имя, отчество)

«К защите допускаю»

Заведующий кафедрой _____ Лепешкин Олег Михайлович

(подпись) (фамилия, имя, отчество)

«____»_____ 20___ г.

Санкт-Петербург

МИНИСТЕРСТВО НАУКИ И ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»

Заведующий кафедрой

_____ _____
(подпись) (фамилия, имя, отчество)

«___»_____20___ года

Задание

на выпускную квалификационную работу

студенту _____
(фамилия, имя, отчество)

1. Тема Создание модели безопасности образовательной организации

закреплена приказом ректора Университета от «____» _____20___ года, № _____

2. Срок сдачи законченной работы «___» _____20___ года

3. Исходные данные к выпускной квалификационной работе:

4. Перечень вопросов, подлежащих разработке (краткое содержание работы:

Введение. Актуальность темы, цели и задачи ВКР

Глава 1 Основы обеспечения безопасности в образовательной организации
(наименование главы)

Глава 2 Разработка аналитико-математической модели принятия решений в системе обеспечения информационной безопасности образовательной организации
(наименование главы)

Глава 3 Методика применения аналитико-математической модели в системе обеспечения информационной безопасности образовательной организации
(наименование главы)

Глава 4 Научно-экономическое обоснование методики построения системы управления информационной безопасностью образовательной организации
(наименование главы)

Заключение. Выводы по работе в целом. Оценка степени решения поставленных задач. Практические рекомендации.

5. Перечень материалов, представляемых к защите:

– Пояснительная записка;

– Схема _____
(наименование схемы)

– Диаграмма _____
(наименование диаграммы)

6. Консультанты по работе

6.1. _____

6.2. _____

…

7. Дата выдачи задания: «__» _____ 20_____ года Руководитель выпускной квалификационной работы

_____ _____
(должность, ученая степень, ученое звание, фамилия, имя, отчество) (подпись)

Задание принял к исполнению «___»_____20___ года

Студент _____ _____
(фамилия, имя, отчество, учебная группа) (подпись)

РЕФЕРАТ

Дипломная работа: _с., ____рис., _табл., __ приложения, ____ источников литературы.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, СТАНДАРТИЗАЦИЯ В ОБЛАСТИ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ, ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, АНАЛИЗ РИСКОВ.

Объект исследования:

Предмет исследования:

Цель работы:

В дипломной работе проводится анализ…

Разработан …

СОДЕРЖАНИЕ

Введение

В условиях стремительной цифровизации образовательной среды информационная безопасность перестала быть технической задачей, превратившись в стратегический приоритет.

Образовательные организации сегодня являются центрами обработки значительных массивов конфиденциальных данных, которые необходимо соответственно защищать. Система безопасности для каждого вуза является сугубо индивидуальной и адаптированной к конкретным условиям.

Актуальность работы обусловлена острой практической необходимостью создания комплексных, адаптивных и экономически обоснованной модели информационной безопасности, специально разработанной с учетом специфики образовательных учреждений. Основной целью информационной сферы является повышение безопасности в том числе в высших учебных заведениях.

В данной работе поставлена и решена задача – произвести анализ угроз в образовательной организации, стандартных средств защиты на основе законодательных актов и создать на основе полученных результатов модель безопасности информации в образовательно организации.

ГЛАВА 1 ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Терминологический анализ безопасности информации в образовательной организации.

Информационная безопасность (ИБ) образовательной организации – это состояние защищенности информационной среды конкретного высшего учебного заведения, обеспечивающее её формирование, использование и развитие в интересах всех участников образовательного процесса [1, с. 45]. В отличие от коммерческих предприятий, целью ИБ вуза является не только сохранение конфиденциальности, целостности и доступности информаци, но и гарантирование непрерывности образовательного процесса, защита академических прав и свобод, а также обеспечение условий для научно-исследовательской деятельности.

Информационная сфера (информационная среда) – это совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений, существующая в рамках конкретного высшего учебного заведения [2, с. 112]. К её ключевым элементам относятся:

-информационные активы: базы персональных данных (ПДн) (абитуриентов, студентов, сотрудников), научные разработки, электронные образовательные ресурсы (ЭОР), финансово-хозяйственная документация, результаты промежуточной и итоговой аттестации.

-информационный источник: локальная вычислительная сеть (ЛВС), серверное оборудование, системы дистанционного обучения (Moodle), официальный сайт, рабочие станции пользователей, системы видеонаблюдения и контроля доступа.

-субъекты информационных отношений: студенты, аспиранты, ППС, АУП, администрация, а также внешние субъекты (Министерство науки и высшего образования, Федеральная служба по надзору в сфере образования и науки (Рособрнадзор), партнёры).

Угроза информационной безопасности вуза – это потенциальная возможность события, которое посредством воздействия на компоненты информационной среды может прямо или косвенно нанести ущерб интересам субъектов информационных отношений в образовательном процессе [3, с. 78].

Изучив открытие источники удалось выделить следующие основые угрозы: [29,?указать ссылку из нескольких источников]

-внешние угрозы**:** компьютерные атаки ransomware), целенаправленные атаки на научные разработки, DDoS-атаки на портал вуза или системе дистанционного обучения в период сессии.

-внутренние угрозы**:** утечки данных по неосторожности сотрудников или обучающихся, преднамеренные действия недовольных студентов (взлом журналов успеваемости), низкая цифровая грамотность пользователей.

-нормативно-правовые угрозы: риск несоответствия требованиям Федерального закона № 152-ФЗ «О персональных данных», Федерального закона № 273-ФЗ «Об образовании в Российской Федерации», отраслевых стандартов ФСТЭК России.

Модель (система) информационной безопасности вуза – это формализованное описание совокупности взаимосвязанных организационных, правовых, технических и кадровых мер, методов и процессов, направленных на достижение и поддержание требуемого уровня защищенности информационной среды высшего учебного заведения. Важнейшими компонентами такой модели являются:

-организационно-правовой компонент: политики и регламенты ИБ, должностные инструкции, система управления инцидентами, план обеспечения непрерывности образовательного процесса.

-технический (программно-аппаратный) компонент: средства защиты информации (межсетевые экраны, системы обнаружения вторжений, антивирусное ПО, системы резервного копирования), обеспечивающие реализацию принципов триады CIA.

-кадровый компонент: программа повышения осведомленности в области ИБ для всех категорий пользователей, специализированная подготовка ответственных сотрудников, формирование культуры безопасного поведения в цифровой среде.

Таким образом, проведенный терминологический анализ позволяет заключить, что построение эффективной модели ИБ для вуза – это комплексная задача, требующая учета его уникальной миссии, структуры информационных активов и угроз. Определенные понятия служат концептуальным фундаментом для последующего анализа рисков и проектирования системы защиты в следующих параграфах работы.

1.2. Развитие подходов к информационной безопасности в образовательных учреждениях.

Данная глава позволит более точно рассмотреть основное направление информационной безопасности в настоящее время, что приведет к более точному построение модели на основе изученных материалов.

Проблема обеспечения информационной безопасности (ИБ) в высших учебных заведениях является комплексной и постоянно развивающей. Её анализ требует рассмотрения в контексте общей эволюции подходов к ИБ, адаптированных к специфике академической среды. Исторически можно выделить несколько этапов, отражающих изменение в системном подходе к информационной безопасности, нормативных требований и понимания угроз [4]

Эволюция подходов к информационной безопасности вуза:

- технократический (инфраструктурный) подход (до середины 2000-х гг.). На ранних этапах цифровизации безопасность в вузах, как и в большинстве организаций, отождествлялась с защитой физической инфраструктуры (серверов, компьютеров) и базовой целостности данных. Основными задачами были обеспечение работоспособности локальных сетей, защита от вирусов и сбоев. Модель строилась по принципу «крепости» с акцентом на периметровую защиту. Человеческий фактор и конфиденциальность информации (кроме явно секретной) часто оставались на втором плане [5].
- нормативно-системный подход (вторая половина 2000-х – 2010-е гг.). Принятие базового законодательства в сфере информации и персональных данных (в России – Федеральные законы № 149-ФЗ и № 152-ФЗ от 2006 года) кардинально изменило парадигму. Вуз стал юридически ответственным оператором персональных данных и субъектом ИБ. Фокус сместился на соответствие (compliance) предписаниям регуляторов. Система ИБ стала строиться «от требований», что зачастую приводило к её бюрократизации и отрыву от реальных образовательных и научных процессов [6].
- риск-ориентированный и интегративный подход (с 2010-х гг. по настоящее время). Рост сложности киберугроз, цифровая трансформация образования и распространение международных стандартов (например, ISO/IEC 27001) сформировали современный взгляд. Безопасность стала рассматриваться как неотъемлемая часть управления вузом, обеспечивающая его устойчивость. Ключевой становится концепция управления рисками ИБ, где меры защиты адекватны потенциальному ущербу для репутации,

финансов и непрерывности деятельности. Цель – интеграция системы менеджмента ИБ (СМИБ) в основные бизнес-процессы университета: образовательный, научный, административный [7].

Концепция триады (конфиденциальность, целостность, доступность). В образовательной среде эта базовая триада приобретает особое значение [8]:

-конфиденциальность (Confidentiality): защита персональных данных студентов и сотрудников, предварительных научных результатов, экспертных заключений, внутренней переписки.

-целостность (Integrity): гарантия неизменности критически важных данных: учебных планов, экзаменационных ведомостей, научных данных, результатов приёмной кампании, финансовой отчетности.

-доступность (Availability): обеспечение бесперебойной работы ключевых сервисов, особенно в пиковые нагрузки (системы дистанционного обучения (СДО), электронные библиотеки, личные кабинеты, сайты).

Концепция «безопасности как процесса». Означает, что ИБ – не разовое мероприятие, а непрерывный цикл (планирование, внедрение, контроль, улучшение). Для вуза это требует постоянной адаптации политик к новым технологиям (облака, IoT), регулярного обучения быстро меняющегося контингента (студенты) и периодической переоценки рисков [9].

Концепция «культуры информационной безопасности». Признаёт человеческий фактор ключевым элементом системы. В условиях высокой ротации (ежегодный приток тысяч первокурсников) и разнородности цифровой грамотности формирование устойчивых безопасных поведенческих паттернов у всех участников образовательного процесса (студенты, ППС, администрация) становится стратегической задачей [10].

Концепция «безопасности по дизайну» (Security by Design). Современная парадигма, требующая встраивания принципов защиты на этапе проектирования новых систем и сервисов (например, цифрового кампуса, платформ для коллаборации). Это позволяет минимизировать уязвимости и затраты на последующие доработки [11].

В научной литературе можно выделить несколько устойчивых направлений исследований информационной безопасности в вузах [12]:

-техническое направление**.**

Разработка и адаптация решений для защиты гетерогенной, открытой и распределённой ИТ-инфраструктуры вуза, включая безопасность Wi-Fi, BYOD (Bring Your Own Device — это политика, при которой сотрудники (или студенты и преподаватели) используют личные мобильные устройства (ноутбуки, смартфоны, планшеты) для работы с корпоративными или учебными ресурсами (интернет-библиотека, работа с облачными сервисами).

-организационно-управленческое направление**.**

Представляет собой поиск моделей эффективного внедрения системы менеджмента информационной безопасности в специфической оргструктуре вуза, оценка экономической эффективности, анализ правовых аспектов (международное сотрудничество, облачные вычисления).

-социально-педагогическое направление**.**

Исследование методологий формирования культуры ИБ, оценка эффективности обучающих программ для разных целевых групп, изучение поведенческих факторов риска.

Для успешного построения модели необходимо рассмотреть законодательно-правовую основу построения безопасности в образовательной организации, так как основной упор должен быть на успешном интегрирование модели, позволяющем не только защититься от угроз, но и обеспечить регламентированность всех действий в вузе.

1.3. Законодательно правовая основа

Деятельность по обеспечению информационной безопасности (ИБ) в российском вузе осуществляется в рамках строго регламентированного правового поля. Нормативная база формирует обязательные требования и задает вектор для построения системы менеджмента информационной безопасности (СМИБ). Её можно структурировать по нескольким уровням.

Международные стандарты и рекомендации (уровень лучших практик):

-ISO/IEC 27001:2022 «Информационная безопасность, кибербезопасность и защита приватности — Системы менеджмента информационной безопасности — Требования». Данный стандарт не является обязательным, но признан мировым эталоном. Он предоставляет вузу методологию для построения риск-ориентированной СМИБ, интегрированной в общие

процессы управления. Его внедрение свидетельствует о зрелости подходов университета к ИБ [7].

-стандарты и рекомендации для образовательных организаций (например, от ассоциаций EDUCAUSE, ENISA). Предлагают адаптированные под академическую среду практики защиты данных, управления идентификацией и реагирования на инциденты.

Федеральный уровень (обязательный для исполнения):

-Конституция Российской Федерации. Статья 23 гарантирует право на неприкосновенность частной жизни, личную и семейную тайну, что является базисом для защиты персональных данных.

-Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Определяет ключевые понятия (информация, информационная система, владелец информации), устанавливает принципы правового регулирования и общие требования к защите информации [6].

-Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (с изм.). Является краеугольным камнем для вуза как для оператора ПДн. Закон устанавливает:

- правовые основания обработки ПДн студентов, абитуриентов, сотрудников.
- требования к содержанию и объему ПДн.
- обязанности оператора по обеспечению конфиденциальности и безопасности ПДн (ст. 19).
- необходимость уведомления Роскомнадзора.

-Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации». Статья 28 возлагает на образовательную организацию ответственность за жизнь и здоровье обучающихся, что в цифровой среде транслируется в обязанность обеспечивать безопасность их персональных данных и цифровую среду обучения.

Требования регуляторов в области ИБ:

-приказы ФСТЭК России (например, № 17, № 21, № 31) – устанавливают требования по защите информации в государственных информационных системах (ГИС), к которым

могут относиться отдельные системы вуза (например, система приема), и требования к организационным мерам.

-приказы ФСБ России (например, № 378, № 66) – регулируют вопросы лицензирования деятельности по технической защите конфиденциальной информации и использования средств криптографической защиты информации (СКЗИ).

-методические документы Роскомнадзора – разъясняют порядок применения 152-ФЗ, требования к уведомлению и проведению проверок.

Локальный уровень (внутренние документы вуза):
На основании федерального законодательства вуз обязан разработать и внедрить пакет организационно-распорядительных документов (ОРД), который является основой его СМИБ. К ним относятся:

-политика информационной безопасности – основной документ, определяющий цели, принципы и подходы.

-концепция (программа) обеспечения ИБ – документ стратегического планирования.

-инструкции и регламенты (по работе с ПДн, по использованию электронной почты и интернета, по реагированию на инциденты ИБ и др.).

-положение о разграничении прав доступа.

-акты классификации информации.

Правовое поле в области ИБ для вуза является многоуровневым и комплексным. Оно сочетает императивные (обязательные) требования федерального законодательства (149-ФЗ, 152-ФЗ) и предписаний регуляторов (ФСТЭК, ФСБ) с рекомендательными международными стандартами (ISO 27001), задающими уровень лучших практик. Задача вуза – не просто формально соответствовать требованиям, а интегрировать их в свою операционную деятельность через систему внутренних локальных нормативных актов. Проблема часто заключается в разрыве между формальным наличием таких документов и их реальным исполнением в условиях академической свободы и открытости, что создает зоны правового и технологического риска.

1.4. Разработка концептуальной модели информационной безопасности для вуза

На основе проведенного анализа теоретических основ, терминологического аппарата, а также законодательной и нормативной базы,

становится возможным построение интегральной концептуальной модели. Эта модель служит абстрактным представлением ключевых сущностей, взаимосвязей и принципов, лежащих в основе организации и обеспечения безопасности в условиях гибридной рабочей среды. Она призвана структурировать проблемное поле и задать рамки для дальнейшего исследования и проектирования конкретных решений.

Концептуальная модель строится на следующих фундаментальных предпосылках, вытекающих из изученных источников:

-центральность информации и активов.

Основным объектом защиты является информационный актив (конфиденциальные данные, персональные данные, интеллектуальная собственность), который циркулирует между субъектами и обрабатывается в различных средах [13, 14].

-принцип минимизации прав (Zero Trust).

В условиях размывания периметра классической модели безопасности принимается постулат о том, что доступ к активам не предоставляется по умолчанию, даже изнутри условного периметра. Каждый запрос на доступ должен быть аутентифицирован, авторизован и непрерывно валидирован [15].

-трехсторонняя система взаимодействия.

Модель выделяет три ключевых компонента, взаимодействие которых необходимо регулировать: Сотрудник (Пользователь), Рабочая среда (Ресурсы), и Организация (Политики и Управление) [16, 17].

-риск-ориентированный подход.

Все управленческие и технические меры выстраиваются не на основе формального соответствия, а на основе постоянной оценки и минимизации рисков, угрожающих конфиденциальности, целостности и доступности (триада CIA) информационных активов [13, 18].

Исходя из этого предлагается следующая многоуровневая концептуальная модель (рис.1).

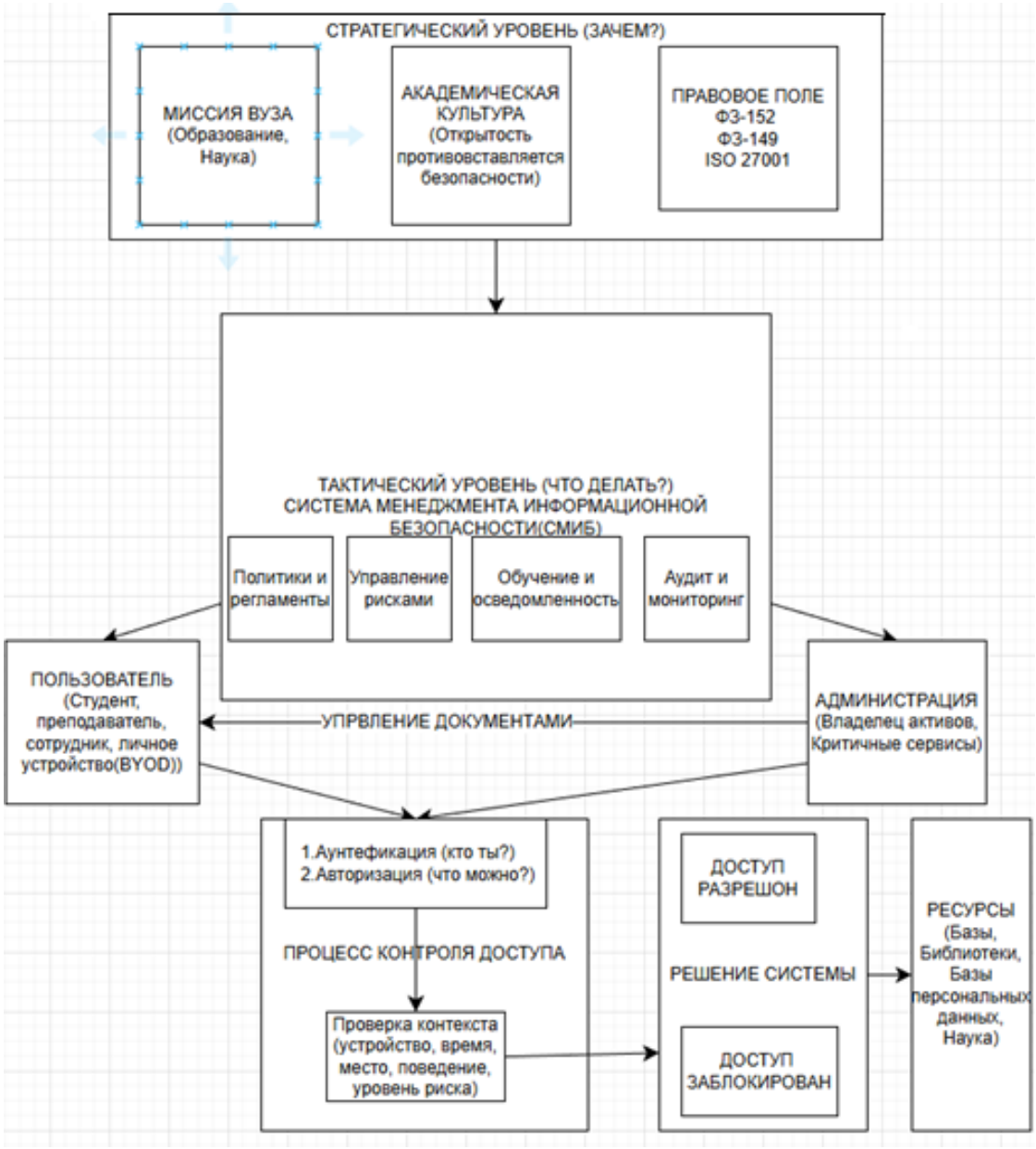


Рисунок №1 – Концептуальная модель информационной безопасности вуза

Описание элементов и взаимосвязей модели.

Стратегический уровень управления. Формирует общий контекст. Цели и корпоративная культура определяют приемлемый уровень риска и приоритеты. Правовое поле (проанализированное в п. 1.3), включая 152-ФЗ, 149-ФЗ и отраслевые требования, задает обязательные ограничения и рамки для всех нижележащих процессов [19, 20, 21, 22].

Тактический уровень политик (Ядро СМИБ).Это уровень, на котором абстрактные принципы и требования преобразуются в конкретные управленческие механизмы. Центральным элементом является Система

менеджмента информационной безопасности (СМИБ), построенная в соответствии с циклом PDCA (Plan-Do-Check-Act) и стандартами, подобными ISO 27001 [13, 18].

Ее ключевые компоненты:

- Политики и регламенты:

Локальные нормативные акты, конкретизирующие, *как* должны работать принципы Zero Trust и требования законодательства применительно к гибридной работе (политика BYOD, политика удаленного доступа) [16, 17].

- Управление доступом (IAM).

Реализует процессы аутентификации и авторизации, обеспечивая принцип наименьших привилегий [15].

- Управление инцидентами (IRP).

Процедуры реагирования на нарушения безопасности [13].

- Обучение и осведомленность.

Непрерывная работа по формированию у Сотрудника культуры безопасности как элемента корпоративной культуры [16].

- Мониторинг и аудит.

Обеспечивает обратную связь для проверки эффективности мер и соответствия [13].

Операционный уровень контроля доступа - это уровень, на котором происходит непосредственное взаимодействие пользователя с ресурсами.

Он функционирует по принципу непрерывного цикла доступа:

Сотрудник с помощью Устройства (корпоративного или личного – BYOD/CYOD) инициирует запрос на доступ к Ресурсу (данным, приложению, сервису) [16, 17].

Аутентификация отвечает на вопрос «Кто ты?», используя многофакторные и, желательно, адаптивные (контекстно-зависимые) методы [15].

Авторизация отвечает на вопрос «Что тебе можно?», проверяя права доступа, основанные на роли пользователя (RBAC) и контексте сессии (устройство, геолокация, время, поведенческие аномалии). Именно здесь реализуется контекстная проверка – ключевой элемент Zero Trust [15].

Ресурсы (Рабочая среда) предоставляются только после успешного прохождения всего цикла. Доступ не является разовым, а постоянно перепроверяется [15].

Взаимосвязи и потоки данных:

- прямая связь (управление) - Политики (тактический уровень) напрямую определяют правила работы механизмов аутентификации и авторизации [13, 16].
- обратная связь (адаптация) - Данные мониторинга с операционного уровня и результаты расследования инцидентов поступают на тактический уровень, что приводит к пересмотру политик, донастройке правил и дополнительному обучению сотрудников. Это закрывает цикл непрерывного улучшения СМИБ [13, 18].

Разработанная концептуальная модель интегрирует ключевые выводы из теоретической и правовой частей исследования. Она визуализирует переход от классической периметровой модели безопасности [14] к архитектуре непрерывного адаптивного контроля доступа, центрированной на данных и идентичности. Модель подчеркивает, что безопасность гибридной работы – это не набор разрозненных технологий, а единая управленческая система, в которой технологические меры (аутентификация, шифрование), организационные меры (политики, обучение) и человеческий фактор (сотрудник) взаимосвязаны и управляются на основе оценки рисков в рамках заданного правового и стратегического контекста. Данная модель служит основой для последующего анализа угроз, выявления уязвимостей и проектирования архитектурных и организационных решений.

Выводы по главе 1

Проведенный анализ позволил установить, что обеспечение информационной безопасности вуза представляет собой комплексную стратегическую задачу, выходящую за рамки чисто технической защиты. В основе эффективной модели лежит понимание уникальной информационной среды учебного заведения, включающей конфиденциальные данные, научные разработки и критически важные образовательные сервисы. Современный подход сместился от простого соблюдения нормативных требований к риск-ориентированному управлению, интегрированному в основные процессы университета. Разработанная концептуальная модель отражает этот подход, объединяя стратегическое управление, тактические политики и операционный контроль в единую адаптивную систему, построенную на принципах Zero Trust и непрерывного улучшения. Данная модель служит основой для последующего анализа угроз,

выявления уязвимостей и проектирования архитектурных и организационных решений.

ГЛАВА 2. РАЗРАБОТКА АНАЛИТИКО-МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРИНЯТИЯ РЕШЕНИЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Обоснование синтеза модели процесса обеспечения информационной безопасности через использование закона сохранения целостности объекта и принципа управленческого решения

В основе защиты информации всегда находится человеческий выбор [23]. Этот выбор осуществляет ответственное лицо, опираясь на собственную логику или формальные правила. Для модели в контексте информационной безопасности, а именно в вопросах анализа, моделирования, оптимизации, совершенствования процессов и механизмов человек в первую очередь стремится к достижению цели управления. Исходя из вышесказанного необходимо рассмотреть модель управленческого решения. Наиболее ярко данная модель представлена в статье Бурлова В.Г. и Грачева М.И..[29]

В данной работе подразумевается схематичное описание состояний системы, которые раскроют его ключевые атрибуты и параметры [23]. Модель даст нам представление управляющего воздействия в области ИБ что приведет к формализованному сценарию работы системы безопасности. Этот сценарий отражает поведение защитного механизма, выполняющего свои главные функции — сохранения конфиденциальности, целостности и доступности данных.

Нужно учитывать, что модель применяется к уже существующим параметрам, ведь для новой системы эти характеристики будут расплывчатыми и будут требовать детальной проработки. Для уверенного достижения поставленных целей необходимо умение проектировать управленческие и технические процедуры с заранее определёнными характеристиками. Однако если неизвестны условия, при которых эти процедуры могут устойчиво функционировать, их невозможно целенаправленно создавать [24, 25]. Невозможность такого проектирования лишает гарантий в достижении результатов по защите информации. Ключ к решению этой принципиальной

задачи заключается в создании строгой методологической основы для построения системы безопасности [26].

В контексте образовательной организации, где информационные ресурсы включают персональные данные, научные разработки и учебные материалы, отсутствие методологических основ приводит к ситуации, когда «результаты деятельности по решению задач функционирования систем обеспечения безопасности не соответствуют ожиданиям лица, принимающего решения». ЛПР (например, руководитель службы ИБ, проректор по ИТ) действует, опираясь на три ключевые категории: Система (комплекс средств и мер ИБ), Модель (её представление) и Предназначение (цели защиты).

Для преодоления указанного разрыва между ожидаемым и реальным результатом в данной работе применяется подход, предложенный В.Г. Бурловым и М.И. Грачевым [27], адаптированный к предметной области ИБ. Вместо традиционного анализа известных уязвимостей предлагается метод синтеза адекватной модели процесса управления ИБ. Основой для синтеза служит закон сохранения целостности объекта (ЗСЦО), который обеспечивает достижение цели функционирования системы. ЗСЦО трактуется как устойчивая, объективная, повторяющаяся связь свойств объекта (системы ИБ) и свойств его действий при фиксированном предназначении [28]. В применении к ИБ это означает, что целостность (как свойство) защищаемой информационной системы и целостность (как свойство) процессов её защиты неразрывно связаны и должны сохраняться на всем жизненном цикле.

Таким образом, для решения задачи управления ИБ необходимо:

1. Синтезировать правильно построенную систему защиты на основе ЗСЦО.
2. Синтезировать адекватную модель процесса её функционирования для ЛПР.

Синтез аналитико-динамической модели процесса управления информационной безопасностью

В соответствии с адаптированным подходом [27], модель функционирования системы обеспечения ИБ образовательной организации основывается на системной интеграции четырех базовых процессов:

-Р1 – Целевой процесс (нормальное функционирование). Состояние, при котором информационная система работает в штатном режиме, а угрозы ИБ отсутствуют или находятся под контролем.

-Р2 – Процесс формирования (проявления) проблемы. Возникновение инцидента информационной безопасности (атака, утечка, сбой). Данный процесс характеризуется средним временем проявления проблемы ($t_{\_иден}$) – интервалом от момента возникновения предпосылок до момента реального воздействия на систему.

-Р3 – Процесс распознавания (обнаружения) проблемы. Деятельность по выявлению и идентификации инцидента ИБ. Ключевой параметр – среднее время обнаружения проблемы ($t_{\_обн}$), которое зависит от качества систем мониторинга (SIEM, IDS) и квалификации персонала SOC.

-Р4 – Процесс устранения (нейтрализации) проблемы. Меры по ликвидации последствий инцидента, восстановлению работоспособности и устранению уязвимостей. Параметр – среднее время нейтрализации проблемы ($t_{\_нейтр}$), определяемое эффективностью регламентов и компетенциями реагирующих специалистов.

Динамика системы описывается переходами между этими состояниями. Эффективность всей системы управления ИБ может быть выражена через показатель, минимизирующий время нахождения системы в уязвимых или атакованных состояниях (Р2 и Р3).

Работа системы информационной безопасности (ИБ) рассматривается как непрерывный процесс смены её состояний. Ключевым критерием её результативности является минимизация периода пребывания в условиях повышенного риска или активного воздействия.

В настоящем исследовании управленческое воздействие формализуется с помощью следующей математической зависимости:

$P = F\ (T_Э, \Delta t_{пп}, \Delta t_{ип}, \Delta t_{нп})$

где:

$\Delta t_{пп}$ — среднее время обнаружения проблемы оператором;

$\Delta t_{ип}$ — среднее время идентификации (определения сути) проблемы;

$\Delta t_{нп}$ — среднее время нейтрализации (устранения) проблемы.

Фундаментальной предпосылкой для реализации любого управляющего воздействия является параметр $T_Э$ — время, необходимый для оценки и прогноза ключевых параметров риска. Визуальная схема данного процесса отражена на рис. 2.

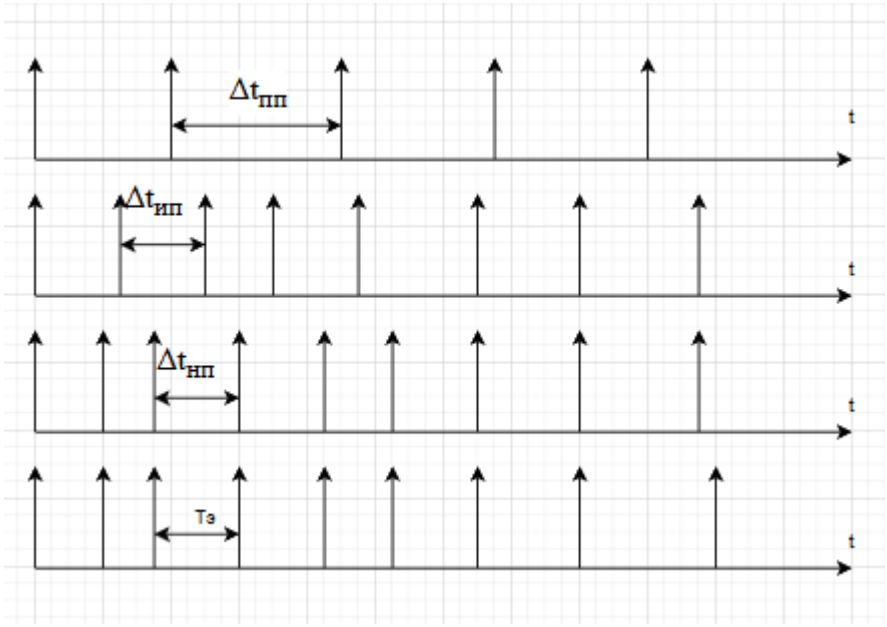
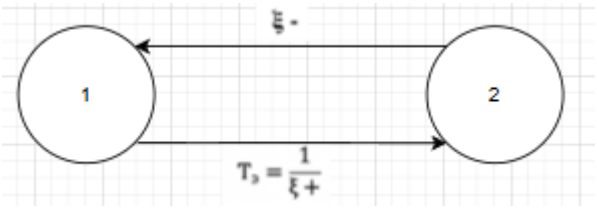


Рисунок №2 – Диаграмма проявления элементов формирования модели решения

Рассмотренные выше четыре процесса, отображённые на диаграммах, описывают общий цикл функционирования.

Базовый цикл жизнедеятельности защищаемой информационной среды может быть представлен в виде упрощённого графа состояний (рис. 3): начальным «1» и конечным «2» (стабильное функционирование, нарушение безопасности).



Рисунок№ 3 – Граф состояний функционирования

На рисунке 3 представлены следующие обозначения:

Тэ = $1/\xi^+$ представляет собой среднее время успешного выполнения запроса, то есть величину, обратную частоте (интенсивности) выполнения запросов (ξ^+).

ξ^- обозначает частоту сбоев, приводящих к неудовлетворению запроса.

Следовательно, параметр ξ^+ характеризует штатный операционный режим, а параметр ξ^- - уровень внешних и внутренних угроз.

Процесс выработки решения в рамках предложенного подхода состоит из последовательных стадий: определение целевого состояния, аккумуляция и обработка данных мониторинга, генерация возможных ответных действий, их экспертиза, финальный выбор и мониторинг результата.

Задача исследования является оптимизация логики функционирования подсистемы реагирования на инциденты ИБ, направленная на сокращение временного лага между моментом возникновения угрозы и началом корректирующих действий. Инструментом для достижения этой цели видится внедрение механизмов автоматизированного управления.

Для реализации такого автоматического управления необходимо:

Установить критерии управляемости целевого процесса.

Спроектировать контур корректирующей обратной связи.

Принципиальная архитектура, воплощающая указанный подход, показана на рисунке 4.

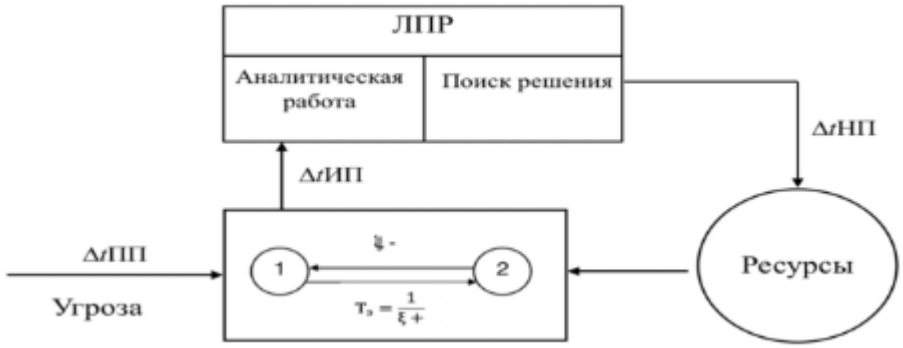


Рисунок №4 Структурная схема функционирования системы

На основе теории марковских процессов и в соответствии с методологией, изложенной в источнике [27], может быть синтезирована математическая модель.

Когда управляемая система пребывает в состоянии 3, на неё воздействует поток угроз с интенсивностью λ. Ключевой задачей на этом этапе является своевременная идентификация угрозы. Специалист по безопасности затрачивает на данный процесс фиксированный интервал времени Δt_ид, в течение которого выполняется первичный анализ и подготовка к мобилизации необходимых ресурсов для противодействия.

В результате успешного анализа система переходит в состояние 4. В этом состоянии угроза не только идентифицирована, но и классифицирована, что позволяет определить оптимальный набор инструментов и процедур для её нейтрализации. Последующий переход из состояния 4 в состояние 2 соответствует фазе активного устранения угрозы и восстановления нормального функционирования. После завершения этого цикла система возвращается в режим ожидания новой угрозы, и процесс детектирования возобновляется.

Возврат системы в исходное (штатное) состояние после устранения инцидента является ключевым индикатором её общей устойчивости и операционной готовности. Интенсивность перехода ξ^{+}, соответствующая переходу из состояния 1 в состояние 2, определяется как величина, обратная среднему времени успешной обработки запроса или выполнения целевой операции. Этот параметр характеризует общую производительность и отзывчивость системы. В противоположность этому, интенсивность ξ^{-}, описывающая переход, связанный с отказом или невыполнением задачи, должна

поддерживаться на статистически минимальном уровне, как правило, не превышающем десятые доли процента.

Эффективность заключительной стадии — нейтрализации угрозы — формализуется через параметр $\nu_2 = 1/\Delta t\_pn$, где Δt_pn — среднее время устранения. Этот параметр является прямой количественной мерой операционной компетентности команды реагирования при работе с нештатными ситуациями. Чем выше значение ν_2, тем быстрее и эффективнее восстанавливается работоспособность системы.

Изложенная логика последовательных переходов между состояниями системы при реагировании на инцидент визуализирована в виде графа состояний, представленного на рисунке 5.

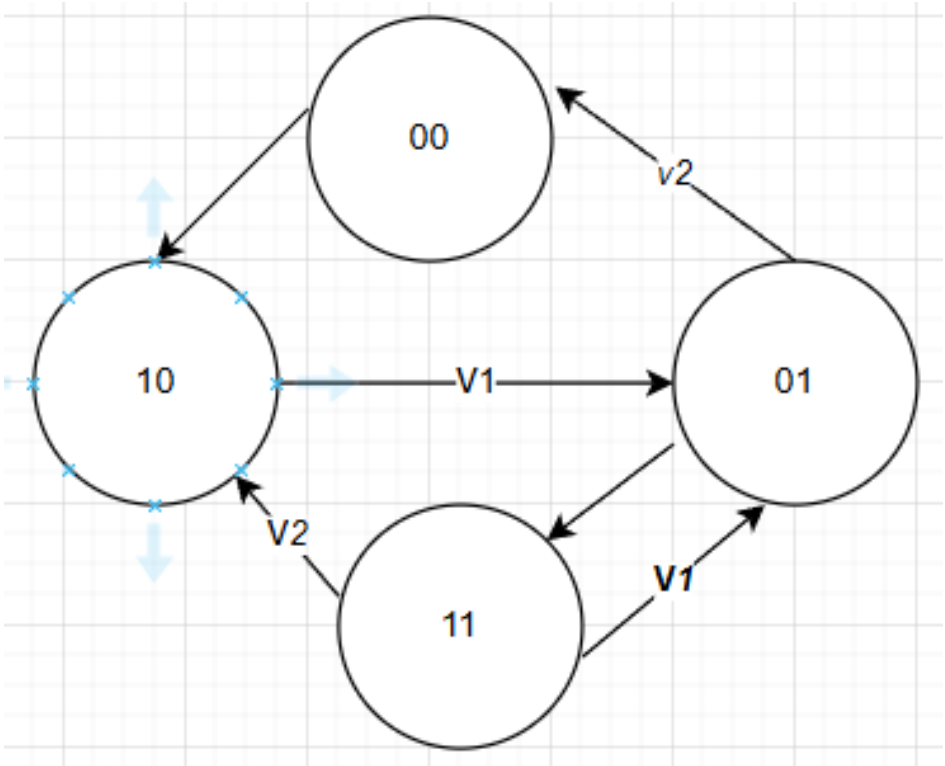


Рисунок №5- Граф состояний, процесса модели управленческого решения ЛПР [27]

Пусть вероятность нахождения системы в состоянии i в момент времени t обозначается как P_i(t). Тогда система дифференциальных уравнений Колмогорова, описывающая динамику, будет иметь вид:

$$\frac{dP_i(t)}{dt} = \sum_{j=1}^{n} {}_{ji}(t) * P_j(t) - P_i(t) * \sum_{j=1}^{n} {}_{ji}(t)$$

где i=0,1, 2,…,n.

Конечная вероятность имеет смысл вычисляться системой линейных алгебраических уравнений, при определенных условиях.

Условия:

1.Производные равны нулю.

2.Уровнения переходят в неизвестные конечные вероятности P_1 , …, P_n.

Нормализующим условием является P0+P1+…+Pn=1.

Системное решение выглядит следующим образом:

$$P_1 = \frac{v_1 * v_2 * \xi^-}{*v_1 * v_2 + *v_1 * \xi^- + *v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-}$$

$$P_2 = \frac{*v_1 * v_2 + v_1 * v_2 * \xi^+}{*v_1 * v_2 + *v_1 * \xi^- + *v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-}$$

$$P_3 = \frac{*v_2 * \xi^-}{*v_1 * v_2 + *v_1 * \xi^- + *v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-}$$

$$P_4 = \frac{*v_1 * \xi^-}{*v_1 * v_2 + *v_1 * \xi^- + *v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-}$$

Вероятность выявления и нейтрализации проблемы емкостью определяется следующей корреляцией:

$$P_2 = \frac{*v_1 * v_2 + v_1 * v_2 * \xi^+}{*v_1 * v_2 + *v_1 * \xi^- + *v_2 * \xi^- + v_1 * v_2 * \xi^+ + v_1 * v_2 * \xi^-}$$

Данное соотношение устанавливает аналитическую зависимость между тремя обобщёнными временными характеристиками процесса реагирования на инцидент:

- времени появления угрозы ($\Delta t_{пп}$),
- времени её идентификации ($\Delta t_{ип}$)
- времени нейтрализации ($\Delta t_{нп}$).

Для анализа этой модели применяется сетевое моделирование, основанное на использовании ориентированных графов. В данной модели вершины графа отображают события, связанные с обнаружением угрозы (например, «инцидент зафиксирован», «угроза идентифицирована»), которые маркируют начало и окончание отдельных этапов работ. Дуги графа соответствуют самим работам или процессам (например, «анализ логов», «применение корректирующих мер»). Выбор сетевой модели в данной работе обусловлен её наглядностью, которая позволяет чётко визуализировать последовательность, взаимосвязь и взаимодействие всех этапов процесса обеспечения информационной безопасности.

↑ - ???

2.1 Проектирование модели образования угроз в образовательном учреждении

Задачей данного этапа проектирования является необходимость связать программно-аппаратную часть с безопасностью системы.

Для построения используется модуль угроз описанных в 1 главе образовательной организации

На рисунке 6 представлены основные векторы угроз в образовательной организации:

1. Программное обеспечение;
2. Аппаратное обеспечение;
3. Ресурсы.

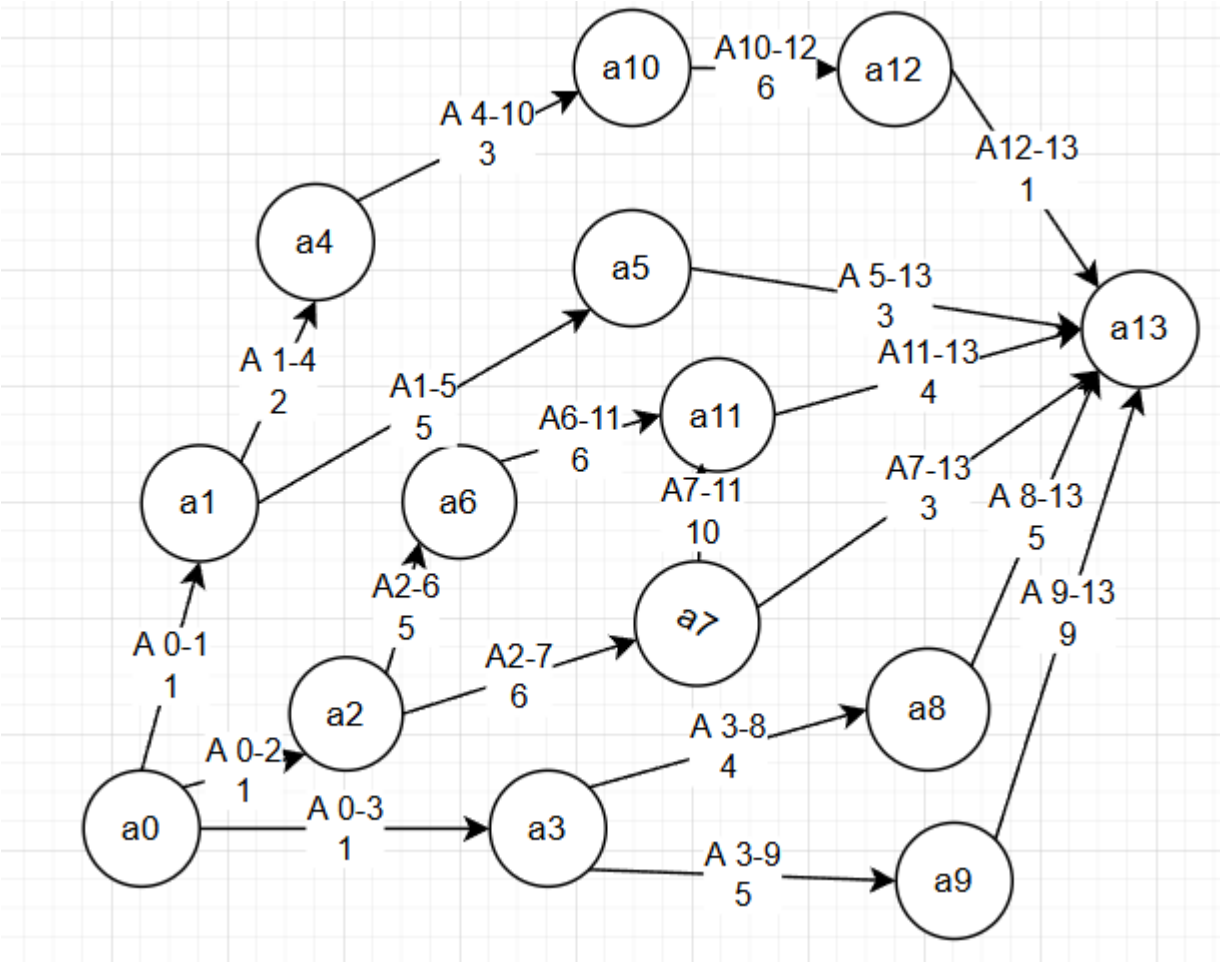


Рисунок №6 – Граф угроз

Угрозы аппаратного обеспечения в образовательном учреждении могут возникать из-за нарушения целостности и управляемости технической подсистемы.

Конкретные причины, вписывающиеся в логику модели:

1. Физический износ и отказы оборудования (естественный процесс, увеличивающий среднее время проявления проблемы t_пр).
2. Недостаточное техническое оснащение (низкий уровень ресурса, что снижает общую устойчивость системы к сбоям).
3. Неквалифицированные действия персонала или учащихся ("человеческий фактор"), ведущие к повреждению аппаратуры.
4. Внешние воздействия (перепады напряжения, климатические факторы), нарушающие работоспособность оборудования.

Угрозы программного обеспечения (ПО) в образовательном учреждении возникают из-за нарушения функциональной целостности и управляемости

информационно-технологической подсистемы. Это приводит к незапланированному переходу системы из состояния нормального функционирования (Р1) в состояние проявленной проблемы (Р2), увеличивая параметр t_пр.

Конкретные причины, соответствующие логике модели:

-уязвимости и ошибки в коде ПО, которые нарушают его "закон сохранения целостности" (ЗСЦО) и делают систему доступной для атак.

-отсутствие или несвоевременное обновление (патчи), что увеличивает временное окно для реализации угрозы.

-использование нелицензионного или непроверенного ПО, вносящее неконтролируемые риски в систему.

-неэффективность подразделения мониторинга, которая увеличивает t_обн, позволяя вредоносной активности развиваться.

Угрозы ресурсам (доступу и информации) в образовательном учреждении возникают из-за нарушения целостности и управляемости информационно-коммуникационной подсистемы. Это ведёт к сбою в достижении цели управления (обеспечение доступности и конфиденциальности информации) и переводу системы в нештатное состояние.

Далее описаны конкретные причины, вписывающиеся в логику модели и термины документа.

Низкая квалификация или злонамеренные действия персонала ("человеческий фактор") — главный внутренний дестабилизирующий фактор. Это может быть разглашение учётных данных, установка, небезопасного ПО, ведущего к утечке, или намеренная передача конфиденциальной информации.

Отсутствие или неадекватность политик управления доступом - признак слабости системы управления. Это приводит к неэффективному распределению прав, увеличивая время обнаружения ($t_{обн}$) и нейтрализации аномалий.

Таблица №1- Перечень событий в модели появления угрозы

Обозначение	Наименование
a0	Угроза

a1	Компрометация периферийного сетевого устройства
a2	Наличие неисправленной уязвимости в сторонней библиотеке
a3	Неэффективная архитектура или "утечка" ресурсов в приложении
a4	Сканирование сети с скомпрометированного устройства
a5	Массовое заражение рабочих станций
a6	Эксплуатация уязвимости через обработанные данные
a7	Повышение привилегий и получение полного контроля над системой
a8	Атаки на уязвимости в программном обеспечении
a9	Отсутствие или неадекватность политик управления доступом
a10	Нарушение законов и уставов по обработке и хранению данных
a11	Установка постоянного вредоносного ПО
a12	Перегрузка и отказ сетевого оборудования
a13	Нарушение работы системы

Таблица №2 – Перечень работ в модели появления угроз

Обозначение работ	Наименование работ	Время выполнения работы, нс	Предшествующие работы	Последующие работы

A 0-1	Фишинговая атака	1	-	A 1-4, A 1-5
A 1-4	Разведка изнутри	2	A 0-1	A 4-10
A 4-10	Поиск, хищение данных	3	A 1-4	A 10-12
A 10-12	Создание помех или маскировка	6	A 4-10	A 12-13
A 12-13	Отказ в обслуживании для пользователей	1	A 10-12	-
A 1-5	Эксплуатация уязвимости в ОС	5	A 0-1	A 5-13
A 5-13	Заражение рабочих станций	3	A 1-5	-
A 0-2	Обнаружение и инвентаризация	1	-	A 2-6, A 2-7
A 2-6	Подготовка и проведение атаки	5	A 0-2	A 6-11

A 6-11	Закрепление в системе	6	A 2-6	A11-13
A11-13	Реализация конечной цели	4	A 6-11	-
A 2-7	выполнения кода	6	A 1-2	A 7-11, A7-13
A 7-11	Внести изменения в систему на самом глубоком уровне	10	A 2-7	A11-13
A11-13	Изменяет настройки оборудования, приводя к его отказу	4	A 7-11	-
A7-13	Целенаправленный саботаж	3	A 2-7	-
A 0-3	Разработка с ошибками или злонамеренное внедрение	1	-	A 3-8, A 3-9
A 3-8	Создание условий для атаки	4	A 0-3	A 8-13

А 8-13	Прямая атака на доступность через уязвимости	5	А 3-8	-
А 3-9	Выявление слабостей процессов	5	А 0-3	А 9-13
А 9-13	Реализация рисков из-за слабого контроля	9	А 3-9	-

Анализ графа угроз безопасности

Ранее время наступления j-го события T_p (j) вычисляемого формулой:

$$T_P(j) = \frac{\max}{i \subset j}(T_P(i) - t_{ij})$$, где:

– i и j обозначаются номера предшествующего и последующего событий;

- t ij – продолжительность (i, j) -й работы.

Из обозначения $i \subset j$ следует, что событие i предшествует событию j.

Таблица №3 – Результаты расчетов сроков совершения событий по графу угроз

Номер события	Сроки свершения события: ранний $t^p(i)$
a0	
a1	1
a2	1
a3	1
a4	3

a5	6
a6	6
a7	7
a8	5
a9	6
a10	6
a11	17
a12	12
a13	21

Самое позднее допустимое время наступления i-го события Тп (i),

Вычисляемое по формуле $T_{П}(j) = \min_{i \supset j}(T_{П}(i) - t_{ij})$

Где из обозначения $i \subset j$ следует, что событие j предшествует событию i

Таблица №4 – Результаты расчетов сроков свершения поздних событий по графу угроз

Номер события	Сроки свершения события: поздний $t^{п}(i)$
a0	0
a1	9
a2	1
a3	7
a4	11
a5	18
a6	11
a7	7
a8	16
a9	12
a10	14
a11	17

a12	20
a13	21

Резерв времени данного события Ri вычисляемый по формуле

$$R_i = (T_П(i) - T_P(i))$$

Таблица №5 – Результаты расчетов резерва времени в модели проявления угроз

№ события	Резерв времени, R(i) наносикунды
a0	0
a1	8
a2	0
a3	6
a4	8
a5	12
a6	5
a7	0
a8	11
a9	6
a10	8
a11	0
a12	8
a13	0

Полный резерв времени работы rп (i.j), вычисляемый по формуле

$$r_П(\mathrm{i,j}) = (T_П(j) - T_P(i) - t_{ij})$$

Таблица №6 – Результаты расчетов полного резерва времени в модели появления угроз

Полный резерв $R^{П}$	Полученное значение
$R^{П}_{(0,1)}$	9-1-0 = 8
$R^{П}_{(0,2)}$	1-1-0 = 0
$R^{П}_{(0,3)}$	7-1-0 = 6
$R^{П}_{(1,4)}$	11-2-1 = 8
$R^{П}_{(1,5)}$	18-5-1 = 12
$R^{П}_{(2,6)}$	11-5-1 = 5
$R^{П}_{(2,7)}$	7-6-1 = 0
$R^{П}_{(3,8)}$	16-4-1 = 11
$R^{П}_{(3,9)}$	12-5-1 = 6
$R^{П}_{(4,10)}$	14-3-3 = 8
$R^{П}_{(5,13)}$	21-3-6 = 12
$R^{П}_{(6,11)}$	17-6-6 = 5
$R^{П}_{(7,11)}$	17-10-7 = 0
$R^{П}_{(8,13)}$	21-5-5 = 11
$R^{П}_{(9,13)}$	21-9-6 = 6
$R^{П}_{(10,12)}$	20-6-6 = 8
$R^{П}_{(11,13)}$	21-4-17 = 0
$R^{П}_{(12,13)}$	21-1-12 = 8

2.2 Модель идентификации безопасности в образовательной организации

Анализ, состоящий из процедур обработки и получения информации по контролю системы и мониторингу, осуществляет сравнение системы с раннее известными результатами, предоставляю вероятные ошибки и сбои системы [23]. Представляя модель контроля состояния системы необходимо составить перечень работ, выполняемых для полного анализа системы на ошибки и время, затраченное на выполнение данных работ.

Таблица №7 – Перечень событий графа идендификации

Обозначение	Наименование событий

a0	Инициация и планирование анализа
a1	Аномальная активность с устройства
a2	Сбор Результатов сканирования уязвимостей
a3	Аномальное потребление ресурсов:
a4	Срабатывание IDS/IPS или фаервола
a5	Корреляция событий от антивируса
a6	Аномалия в логах приложения
a7	Аудит событий безопасности
a8	Срабатывание сигнатур IDS/IPS
a9	Результат аудита доступа
a10	Результат compliance-проверки
a11	Обнаружение EDR/антивирусом персистентного механизма
a12	Срабатывание систем мониторинга сети
a13	Массовые инциденты от пользователей и срабатывание мониторинга
a14	Документирование и блокировка включая рабочее место

На рисунке 7 представлены основные векторы идентификации в образовательной организации:

1. Программное обеспечение;
2. Аппаратное обеспечение;

3. Ресурсы.

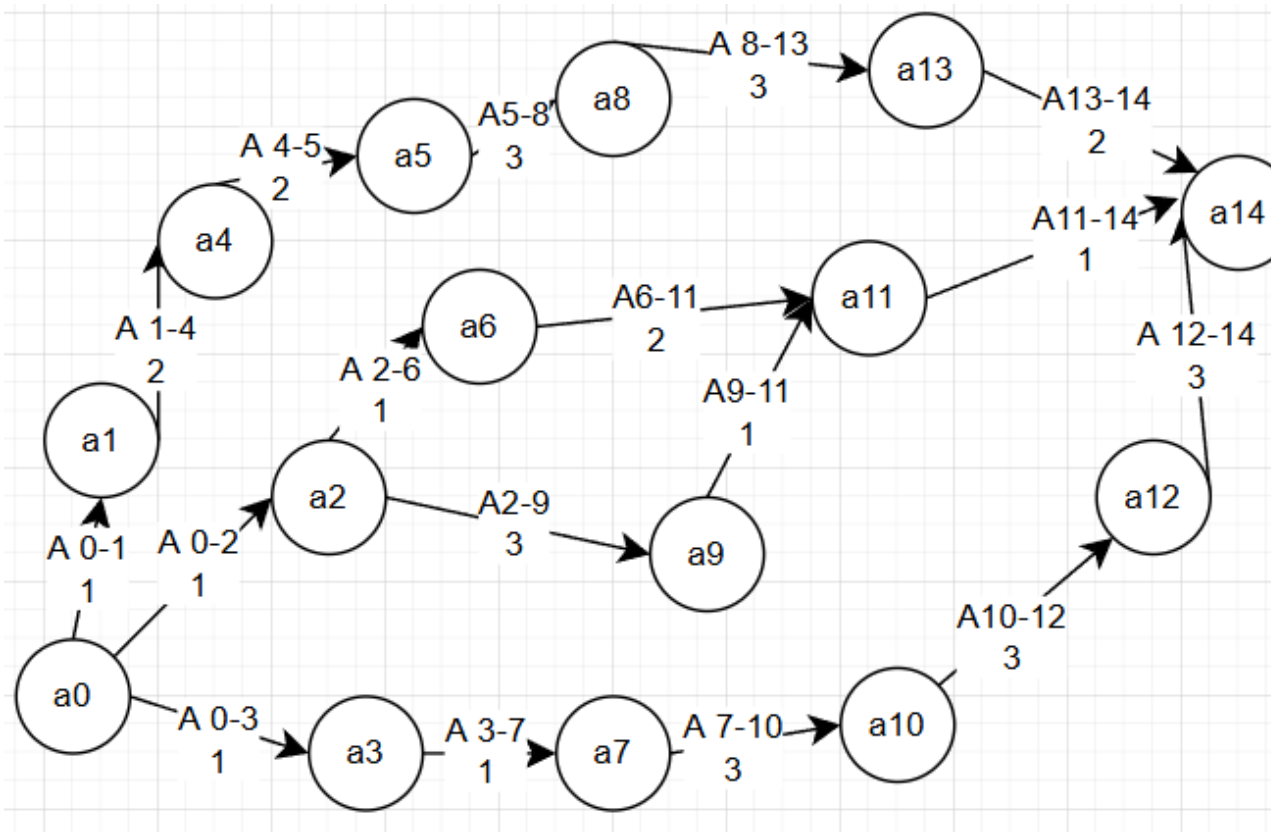


Рисунок 7 – Граф контроля безопасности

Идентификация угроз аппаратного обеспечения в образовательном учреждении фокусируется на своевременном распознавании признаков, указывающих на потенциальный или начавшийся переход системы из состояния нормального функционирования (P1) в состояние проявления проблемы (P2). Ключевая задача — минимизировать время идентификации ($t_{обн}$) для данных классов угроз [24].

Ключевые объекты и признаки для идентификации:

-признаки физического износа и предотказного состояния оборудования: Мониторинг параметров (шум, нагрев, ошибки чтения/записи) для прогнозирования отказа до его наступления и увеличения $t_{пр}$ (времени на реагирование).

-индикаторы недостаточного технического оснащения: Идентификация производится через анализ метрик нагрузки (загрузка ЦП, память, сеть) и частоты сбоев в условиях пиковых учебных нагрузок, что указывает на исчерпание ресурса системы [25].

-паттерны неквалифицированных или ошибочных действий пользователей: Фиксация аномальных действий (частые неправильные выключения, физическое воздействие на устройства) через журналы событий и отчеты персонала как триггеров для перехода в состояние Р2.

-маркеры внешних дестабилизирующих воздействий: Использование данных с датчиков (источники бесперебойного питания, логгеры температуры/влажности) для идентификации угрозы до момента выхода оборудования из строя.

-идентификация угроз программного обеспечения (ПО) заключается в обнаружении отклонений от штатного функционирования информационно-технологической подсистемы, ведущих к нарушению её целостности. Цель — выявить факторы, увеличивающие параметр t_пр (время до проявления проблемы) и t_обн (время её обнаружения) [26].

Ключевые объекты и признаки для идентификации:

-идентификация уязвимостей и признаков эксплуатации ошибок: Регулярный анализ данных сканеров безопасности и SIEM-систем на предмет выявления известных уязвимостей (CVE) и аномальной активности, нарушающей (ЗСЦО) [27].

-индикаторы устаревшего и неподдерживаемого ПО: Автоматизированный инвентаризационный учёт версий ПО и отсутствующих обновлений безопасности для идентификации «окна уязвимости».

-маркеры использования нелегитимного или рискованного ПО: Обнаружение приложений без цифровых подписей, с хеш-суммами, не прошедшими верификацию, или из непроверенных источников.

-признаки неэффективности подсистемы мониторинга**:** Анализ полноты лог-записей, времени реакции на инциденты и количества пропущенных угроз для оценки адекватности идентификации и снижения t_обн.

Идентификация угроз ресурсам (доступу и информации) нацелена на распознавание аномалий и инцидентов в информационно-коммуникационной

подсистеме, которые свидетельствуют о сбое в достижении целей управления конфиденциальностью и доступностью [28].

Ключевые объекты и признаки для идентификации:

-идентификация инсайдерских угроз и действий персонала. Выявление поведенческих аномалий (доступ в нерабочее время, массовая загрузка данных, попытки эскалации привилегий) с помощью систем UEBA (User and Entity Behavior Analytics) как ключевого механизма для обнаружения «человеческого фактора».

-обнаружение слабостей в политиках и механизмах управления доступом. Регулярный аудит назначенных прав (принцип наименьших привилегий), анализ неиспользуемых учётных записей и случаев нарушения процедур доступа для оценки адекватности системы управления и предотвращения роста t_обн.

-маркеры утечки или несанкционированного доступа к информации. Мониторинг каналов передачи данных (почта, облачные сервисы, внешние накопители) на предмет передачи конфиденциальных данных, а также анализ логов доступа к критичным информационным активам.

Таблица №8 – Перечень работ графа идентификации

Обозначение работ	Наименование работ	Время выполнения работ	Предшествующие работы	Последующие работы
А 0-1	инициируется детальный разбор событий	1	-	А 1-4
А 1-4	система обнаружения угроз (IDS/IPS, фаервол) срабатывает	2	А 0-1	А 4-5

A 4-5	Происходит автоматическая или ручная корреляция	2	A 1-4	A 5-8
A 5-8	Решение положительная или отрицательная корреляция	3	A 4-5	A 8-13
A 8-13	Сбор данных пользователей и обработка	3	A 5-8	A 13-14
A 13-14	автоматическая или ручная фиксация событий	2	A 8-13	-
A 0-2	проводится сканирование системы	1	-	A 2-6, A 2-9
A 2-6	аномалии фиксируются	1	A 0-2	A 6-11
A 2-9	На основании итогов проверяется	3	A 0-2	A 9-11
A 6-11	возможное наличие	2	A 2-6	A 11-14

	скрытых или постоянных механизмов			
A 9-11	выявляются несанкционированные или подозрительные изменения	1	A 2-9	A 11-14
A 11-14	фиксация и документирование признаков наличия вредоносных элементов	1	A 9-14, A 6-11	-
A 0-3	Выявление потребления ресурсов	1	-	A 3-7
A 3-7	Запуск аудита событий безопасности для поиска причин	1	A 0-3	A 3-7
A 7-10	Выявление несоответствий	3	A 3-7	A 7-10
A 10-12	Выявление	3	A 7-10	A 10-12

	подозрительных активностей			
А 12-14	Отправка отчета для блокировки	3	А 10-12	-

Анализ графа контроля безопасности

Ранее время наступления j-го события Тр (j) вычисляемого формулой:

$$T_P(j) = \frac{\max}{i \subset j}(T_P(i) - t_{ij})$$, где:

– i и j обозначаются номера предшествующего и последующего событий;

- t ij – продолжительность (i, j) -й работы.

Из обозначения $i \subset j$ следует, что событие i предшествует событию j.

Таблица №9 – Результаты расчетов сроков свершения события (ранний) графе идентификации

Номер события	Сроки свершения события: ранний $t^p(i)$
a0	
a1	1
a2	1
a3	1
a4	3
a5	5
a6	2
a7	2
a8	8
a9	4
a10	5
a11	5

a12	8
a13	11
a14	13

Самое позднее допустимое время наступления i-го события Тп (i),

Вычисляемое по формуле $T_П(j) = \min_{i \supset j}(T_П(i) - t_{ij})$

Где из обозначения : $i \subset j$ следует, что событие j предшествует событию i

Таблица №10 – Результаты расчетов

Номер события	Сроки свершения события: поздний $t^п(i)$
a0	0
a1	1
a2	8
a3	3
a4	3
a5	5
a6	10
a7	4
a8	8
a9	11
a10	7
a11	12
a12	10
a13	11
a14	13

Резерв времени данного события Ri вычисляемый по формуле

$$R_i = (T_П(i) - T_P(i))$$

Таблица №11 – Результаты расчетов

Номер события	Резерв времени, R(i)
a0	0
a1	0
a2	7
a3	2
a4	0
a5	0
a6	8
a7	2
a8	0
a9	7
a10	2
a11	7
a12	2
a13	0
a14	0

Полный резерв времени работы rп (i.j), вычисляемый по формуле

$$r_{П}(\mathrm{i},\mathrm{j}) = (T_{П}(j) - T_{P}(i) - t_{ij})$$

Таблица №12 – Результаты расчетов

Полный резерв $R^{П}$	Полученное значение
$R^{П}_{(0,1)}$	1-1-0 = 0
$R^{П}_{(0,2)}$	8-1-0 = 7
$R^{П}_{(0,3)}$	3-1-0 = 2
$R^{П}_{(1,4)}$	3-2-1 = 0
$R^{П}_{(2,6)}$	10-1-1 = 8
$R^{П}_{(2,9)}$	11-3-1 = 7
$R^{П}_{(3,7)}$	4-1-1 = 2
$R^{П}_{(4,5)}$	5-2-3 = 0

$R^{П}_{(5,8)}$	8-3-5 = 0
$R^{П}_{(6,11)}$	12-2-2 = 8
$R^{П}_{(7,10)}$	7-3-2 = 2
$R^{П}_{(8,13)}$	11-3-8 = 0
$R^{П}_{(9,11)}$	12-1-4 = 7
$R^{П}_{(10,12)}$	10-3-5 = 2
$R^{П}_{(11,14)}$	13-1-5 = 7
$R^{П}_{(12,14)}$	13-3-8 = 2
$R^{П}_{(13,14)}$	13-2-11 = 0

2.3 Модель нейтрализации угроз в образовательной организации

Рассмотрим работы, необходимые для полного устранения выявленных угроз. На рисунке 8 представлены основные векторы нейтрализации угроз в образовательной организации:

1. Программное обеспечение;
2. Аппаратное обеспечение;
3. Ресурсы.

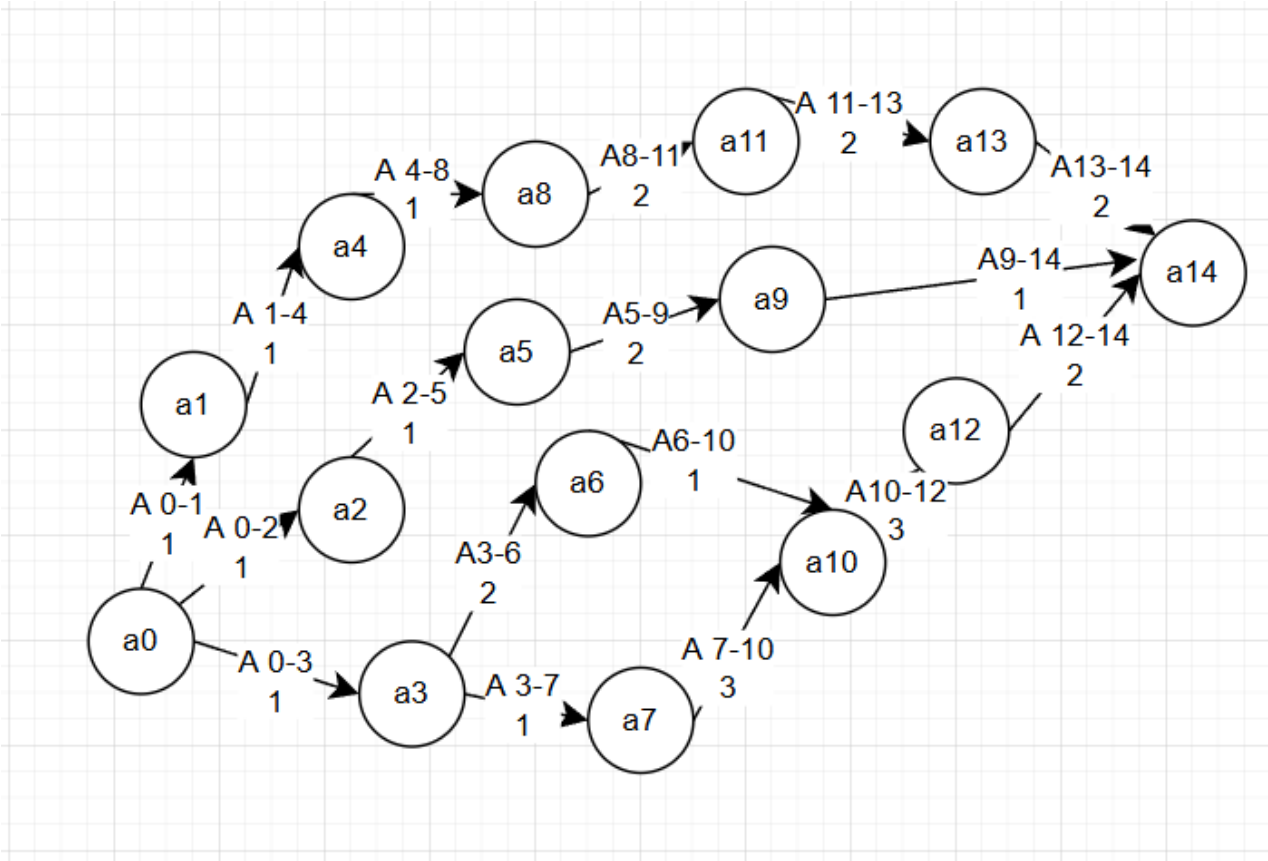


Рисунок №8 – Граф нейтрализации угроз

Нейтрализация угроз аппаратного обеспечения в образовательном учреждении направлена на минимизацию последствий и восстановление технической подсистемы.

Меры нейтрализации:

-профилактика и смягчение последствий физического износа. Внедрение графика планово-предупредительного ремонта и замены оборудования по истечении срока службы для увеличения t_пр. Создание и поддержание фонда запасных частей и готового к работе резервного оборудования для оперативного восстановления.

-компенсация недостаточного технического оснащения. Оперативное перераспределение ресурсов (например, использование мобильных компьютерных классов).Приоритизация задач и временное ограничение некритичных сервисов для поддержания работы ключевых систем.

-корректировка последствий действий персонала и учащихся. Четкие регламенты и инструкции по физическому обращению с техникой. Организация

оперативного ремонта силами IT-специалистов или по гарантии для минимизации времени восстановления.

защита от внешних воздействий. Применение устройств бесперебойного питания (ИБП) и стабилизаторов для нейтрализации перепадов напряжения. Использование климатического оборудования (кондиционеры, осушители) для поддержания допустимых условий эксплуатации.

Нейтрализация угроз программного обеспечения (ПО) заключается в устранении уязвимостей, восстановлении функциональности и целостности информационно-технологической подсистемы после инцидента. Основные задачи — ликвидировать причину перехода в состояние Р2 и восстановить соблюдение «закона сохранения целостности объекта» (ЗСЦО).

Меры нейтрализации:

-устранение уязвимостей и ошибок:

Срочное применение патчей и обновлений безопасности.

Временное отключение уязвимых сервисов или настройка дополнительных правил фильтрации (брандмауэры, WAF) до выпуска фикса.

-восстановление после инцидентов, вызванных устаревшим ПО:

Принудительный запуск централизованного обновления на всех узлах.

Откат к последней стабильной и защищенной версии ПО.

-ликвидация рисков от нелегитимного ПО:

Принудительное удаление нелицензионного и непроверенного программного обеспечения.

Восстановление систем из «чистых» резервных копий, созданных до момента установки проблемного ПО.

-повышение эффективности мониторинга для ускорения реакции:

Настройка автоматических ответов (например, изоляция зараженного хоста в сети) по сигналам SIEM-систем для сокращения t_обн и времени нейтрализации.

Проведение учебных тревог и анализ реальных инцидентов для отработки и ускорения процедур реагирования.

Нейтрализация угроз ресурсам (доступу и информации) фокусируется на пресечении несанкционированных действий, восстановлении контроля и ликвидации последствий утечек. Цель — восстановить достижение цели управления (конфиденциальность и доступность) после сбоя.

Меры нейтрализации:

-реакция на инсайдерские угрозы и действия персонала. Немедленный отзыв или блокировка скомпрометированных учетных записей. Принудительная смена паролей и ключей доступа для всей группы риска. Юридические и дисциплинарные меры в отношении виновных.

-корректировка слабостей системы управления доступом. Срочный пересмотр и ужесточение политик доступа (принцип наименьших привилегий). Отзыв избыточных прав и удаление «мертвых» учетных записей для сокращения поверхности атаки и уменьшения t_обн для будущих аномалий.

-ликвидация последствий утечки информации. Уведомление затронутых лиц и регуляторов (если требуется).

-технические меры. Отзыв документов, шифрование данных, блокировка каналов утечки.Начало расследования для установления полного масштаба инцидента и предотвращения повторения.

Таблица №13 Перечень событий нейтрализации угроз

Обозначение	Наименование событий
a0	Обнаружение
a1	Изоляция
a2	Приоритизация
a3	Остановка
a4	Блокировка
a5	Содержание

a6	Блокировка атаки
a7	Немедленный отзыв учетной записи и лешение прав
a8	Блокировка атаки
a9	Корректировка прав
a10	Немедленное исправление
a11	Изоляция и удаление
a12	Перераспределение нагрузки
a13	Активация плана
a14	Устранение

Таблица №14 Перечень работ нейтрализации угроз

Обозначение работ	Наименование работ	Время выполнения работ	Предшествующие работы	Последующие работы
А 0-1	Предотвращение распространения	1	-	А 1-4
А 1-4	Блокировка активности	1	А 0-1	А 4-8
А 4-8	Конкретизация и применение правил	1	А 1-4	А 8-11

A 8-11	Очистка зараженной системы	2	A 4-8	A 11-13
A 11-13	Переход к восстановлению	2	A 8-11	A 13-14
A 13-14	Восстановление и возврат к нормальной работе	2	A 11-13	-
A 0-2	Оценка критичности	1	-	A 2-5
A 5-9	Анализ первопричины и исправление уязвимостей в управлении доступом.	2	A 2-5	A 9-14
A 9-14	завершение цикла реагирования через системные изменения	1	A 5-9	-
A 0-3	Немедленное прерывание атаки	1	-	A 3-6, A 3-7
A 3-6	Фиксация и предотвращение рестарта	2	A 0-3	A 6-10

А 6-10	Ликвидация уязвимости	1	А 3-6	А 10-12
А 3-7	Реагирование на компрометацию учетной записи	1	А 0-3	А 7-10
А 10-12	Восстановление доступности сервиса	3	А 6-10, А7-10	А 12-14
А 12-14	Завершение восстановительных работ	2	А 10-12	-

Анализ графика нейтрализации угроз

Ранее время наступления j-го события Тр (j) вычисляемого формулой:

$$T_p(j) = \frac{\max}{i \subset j}(T_p(i) - t_{ij})$$,где:

– i и j обозначаются номера предшествующего и последующего событий;

- t ij – продолжительность (i, j) -й работы.

Из обозначения $i \subset j$ следует, что событие i предшествует событию j.

Номер события	Сроки свершения события: ранний $t^p(i)$
a0	
a1	1
a2	1
a3	1
a4	2

a5	2
a6	3
a7	2
a8	3
a9	4
a10	5
a11	5
a12	8
a13	7
a14	10

Таблица №15 – Результаты расчетов

Самое позднее допустимое время наступления i-го события Тп (i),

Вычисляемое по формуле $T_п(j) = \min_{i \supset j}(T_п(i) - t_{ij})$

Где из обозначения $i \subset j$ следует, что событие j предшествует событию i

Таблица №16 – Результаты расчетов

Номер события	Сроки свершения события: поздний $t^п(i)$
a0	0
a1	2
a2	6
a3	1
a4	3
a5	7
a6	4
a7	2
a8	4
a9	9
a10	5
a11	6

a12	8
a13	8
a14	10

Резерв времени данного события Ri вычисляемый по формуле

$$R_i = (T_П(i) - T_P(i))$$

Таблица №17 – Результаты расчетов

Номер события	Резерв времени, R(i)
a0	0
a1	1
a2	5
a3	0
a4	1
a5	5
a6	1
a7	0
a8	1
a9	5
a10	0
a11	1
a12	0
a13	1
a14	0

Полный резерв времени работы rп (i.j), вычисляемый по формуле

$$r_П(\mathrm{i,j}) = (T_П(j) - T_P(i) - t_{ij})$$

Таблица №17 – Результаты расчетов

Полный резерв $R^П$	Полученное значение
$R^П_{(0,1)}$	2-1-0 = 1

$R^{П}_{(0,2)}$	6-1-0 = 5
$R^{П}_{(0,3)}$	1-1-0 = 0
$R^{П}_{(1,4)}$	3-1-1 = 1
$R^{П}_{(2,5)}$	7-1-1 = 5
$R^{П}_{(3,6)}$	4-2-1 = 1
$R^{П}_{(3,7)}$	2-1-1 = 0
$R^{П}_{(4,8)}$	4-1-2 = 1
$R^{П}_{(5,9)}$	9-2-2 = 5
$R^{П}_{(6,10)}$	5-1-3 = 1
$R^{П}_{(7,10)}$	5-3-2 = 0
$R^{П}_{(8,11)}$	6-2-3 = 1
$R^{П}_{(9,14)}$	10-1-4 = 5
$R^{П}_{(10,12)}$	8-3-5 = 0
$R^{П}_{(11,13)}$	8-2-5 = 1
$R^{П}_{(12,14)}$	10-2-8 = 0
$R^{П}_{(13,14)}$	10-2-7 = 1

2.4 Модель функционирования образовательной организации

На рисунке 9 представлены основные векторы функционирования в образовательной организации:

1. Программное обеспечение;
2. Аппаратное обеспечение;
3. Ресурсы.

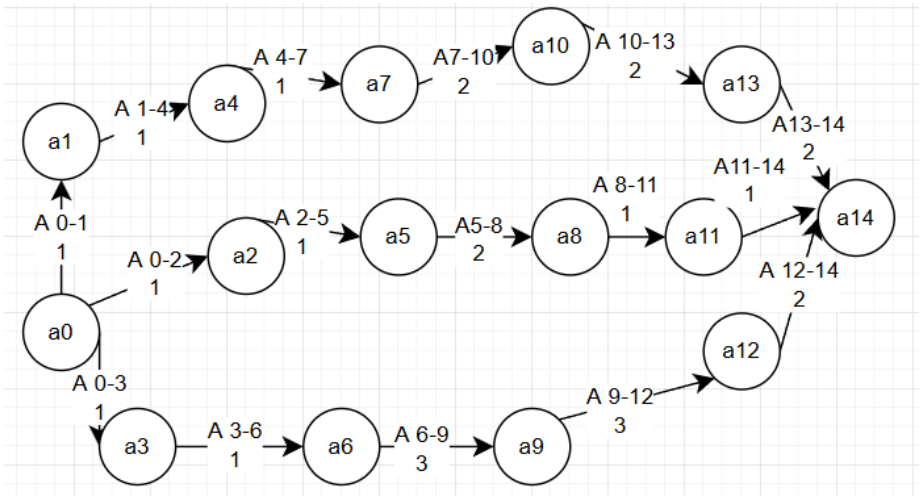


Рисунок №9 - Граф функционирования

Обеспечение функционирования аппаратного обеспечения в образовательном учреждении направлено на поддержание целостности и управляемости технической подсистемы для сохранения её в состоянии нормального функционирования (P1) и предотвращения перехода в состояние, в котором проявляются проблемы (P2). Ключевая задача — максимизировать среднее время безотказной работы (t_пр) за счёт управления ресурсом и устойчивостью системы.

Принципы и процессы штатного функционирования:

-управление жизненным циклом оборудования: Плановые замены и обслуживание для компенсации физического износа, что позволяет прогнозируемо увеличивать t_пр и предотвращать внезапные отказы.

-уланирование и обеспечение достаточного уровня технического оснащения: Регулярный аудит и пополнение ресурсной базы для поддержания запаса устойчивости системы к пиковым нагрузкам и внутренним сбоям.

-эксплуатация оборудования в рамках регламентов: Обучение пользователей и внедрение инструкций по корректной работе с аппаратурой для минимизации «человеческого фактора» как причины выхода из состояния P1.

-обеспечение стабильной внешней среды: Использование защитной инфраструктуры (ИБП, климат-контроль) для нейтрализации внешних

дестабилизирующих воздействий и поддержания работоспособности оборудования.

Обеспечение функционирования программного обеспечения (ПО) заключается в поддержании функциональной целостности и управляемости информационно-технологической подсистемы. Цель — обеспечить непрерывное соблюдение «закона сохранения целостности объекта» (ЗСЦО) и предотвратить незапланированный переход в состояние Р2.

Принципы и процессы штатного функционирования:

-управление целостностью ПО: Регулярный аудит кодовой базы, использование подписанных дистрибутивов и выполнение политик безопасной разработки (Security by Design) для изначального соблюдения ЗСЦО.

-цикл регулярного обслуживания и обновления: Централизованное и автоматизированное управление установкой патчей и обновлений безопасности для минимизации «окна уязвимости» и поддержания системы в защищенном состоянии Р1.

-управление программными активами: Строгий контроль за устанавливаемым ПО через использование утверждённых репозиториев и лицензионного соглашения, что исключает внесение неконтролируемых рисков.

=эффективная работа подсистемы мониторинга: Настройка проактивного обнаружения аномалий и автоматических оповещений для минимизации времени $t_{обн}$, что позволяет реагировать на отклонения до перехода системы в состояние Р2.

Обеспечение функционирования ресурсов (доступа и информации) сосредоточено на непрерывном поддержании целостности и управляемости информационно-коммуникационной подсистемы для гарантированного достижения цели управления - доступности и конфиденциальности информации.

Принципы и процессы штатного функционирования:

-управление «человеческим фактором» как ресурсом: Постоянное обучение и повышение осведомлённости (Security Awareness) персонала, а также

внедрение культуры информационной безопасности для превращения персонала из фактора риска в элемент защитной системы.

-функционирование системы управления доступом на основе политик: Реализация и регулярный пересмотр политик контроля доступа (например, принцип наименьших привилегий), что обеспечивает эффективное распределение прав, снижает поверхность атаки и ускоряет обнаружение ($t\_{обн}$) любых аномалий.

-штатный мониторинг и контроль информационных потоков: Регулярный аудит логов доступа, использование систем DLP (Data Loss Prevention) для предотвращения утечек и шифрование критичных данных — как рутинные процессы, поддерживающие систему в целевом состоянии P1.

Таблица №18 – Перечень событий функционирования

Обозначение	Наименование событий
a0	Запуск системы образовательной организации
a1	регулярное обновление прошивок
a2	Автоматическое сканирование уязвимостей
a3	Мониторинг производительности
a4	Функционирование антивируса в режиме мониторинга
a5	Логирование запросов к приложению
a6	Ведение журналов аудита (Active Directory)
a7	Событие IDS/IPS с актуальными сигнатурами
a8	Периодический автоматизированный аудит доступа

a9	Периодический автоматизированный аудит доступа
a10	Классификация данных по режиму доступа
a11	контроль целостности файлов
a12	Мониторинг состояния устройств
a13	Мониторинг доступности сервисов
a14	Успешное функционирование

Таблица №19 – Перечень работ функционирования

Обозначение работ	Наименование работ	Время выполнения работ	Предшествующие работы	Последующие работы
А 0-1	Поддержка актуальности	1	-	А 1-4
А 1-4	Обновления прошивок	1	А 0-1	А 4-7
А 4-7	Пассивный сетевой мониторинг	1	А 1-4	А 7-10
А 7-10	Управление жизненным циклом информации и	2	А 4-7	А 10-13

	настройка политик			
A 10-13	Контроль уровня обслуживания	2	A7-10	A 13-14
A 13-14	Подтверждение соответствия рабочих показателей	2	A 10-13	-
A 0-2	Превентивная инвентаризация и оценка рисков	1	-	A 2-5
A 2-5	Сбор аналитики	1	A 0-2	A 5-8
A 5-8	Сверка журналов событий	2	A 2-5	A 8-11
A 8-11	Документирование изменений	1	A5-8	A 11-14
A 11-14	Верификация стабильности	1	A 8-11	-
A 0-3	Наблюдение за утилизацией ресурсов	1	-	A 3-6

А 3-6	Корреляция нагрузки	1	А 0-3	А6-9
А6-9	Периодический автоматизированный аудит доступа	3	А 3-6	А 9-12
А 9-12	Инвентаризация и контроль соответствия конечных точек политикам	3	А 6-9	А 12-14
А 12-14	Обеспечение единообразия и стабильности клиентской среды	2	А 9-12	-

Анализ графа функционирования безопасности

Ранее время наступления j-го события Тр (j) вычисляемого формулой:

$$T_P(j) = \frac{\max}{i \subset j}(T_P(i) - t_{ij})$$, где:

– i и j обозначаются номера предшествующего и последующего событий;

- t ij – продолжительность (i, j) -й работы.

Из обозначения $i \subset j$ следует, что событие i предшествует событию j.

Таблица №20 – Результаты расчетов

Номер события	Сроки свершения события: ранний $t^p(i)$
а0	

a1	1
a2	1
a3	1
a4	2
a5	2
a6	2
a7	3
a8	4
a9	5
a10	5
a11	5
a12	8
a13	7
a14	10

Самое позднее допустимое время наступления i-го события Тп (i),

Вычисляемое по формуле $T_П(j) = \min_{i \supset j}(T_П(i) - t_{ij})$

Где из обозначения : $i \subset j$ следует, что событие j предшествует событию i

Таблица №21 – Результаты расчетов по графу функционирования

Номер события	Сроки свершения события: поздний $t^{п}(i)$
a0	0
a1	2
a2	5
a3	1
a4	3
a5	6
a6	2
a7	4
a8	8

a9	5
a10	6
a11	9
a12	8
a13	8
a14	10

Резерв времени данного события Ri вычисляемый по формуле

$$R_i = (T_П(i) - T_P(i))$$

Таблица №22 – Результаты расчетов

Номер события	Резерв времени, R(i)
a0	0
a1	1
a2	4
a3	0
a4	1
a5	4
a6	0
a7	1
a8	4
a9	0
a10	1
a11	4
a12	0
a13	1
a14	0

Полный резерв времени работы rп (i.j), вычисляемый по формуле

$$r_П(\mathrm{i,j}) = (T_П(j) - T_P(i) - t_{ij})$$

Таблица №23 – Результаты расчетов по графу функционированию

Полный резерв $R^{П}$	Полученное значение
$R^{П}_{(0,1)}$	2-1-0 = 1
$R^{П}_{(0,2)}$	5-1-0 = 4
$R^{П}_{(0,3)}$	1-1-0 = 0
$R^{П}_{(1,4)}$	3-1-1 = 1
$R^{П}_{(2,5)}$	6-1-1 = 4
$R^{П}_{(3,6)}$	2-1-1 = 0
$R^{П}_{(4,7)}$	4-1-2 = 1
$R^{П}_{(5,8)}$	8-2-2 = 4
$R^{П}_{(6,9)}$	5-3-2 = 0
$R^{П}_{(7,10)}$	6-2-3 = 1
$R^{П}_{(8,11)}$	9-1-4 = 4
$R^{П}_{(9,12)}$	8-3-5 = 0
$R^{П}_{(10,13)}$	8-2-5 = 1
$R^{П}_{(11,14)}$	10-1-5 = 4
$R^{П}_{(11,14)}$	10-2-8 = 0
$R^{П}_{(12,14)}$	10-2-7 = 1
$R^{П}_{(13,14)}$	10-2-7 = 1

2.5 Соответствие математической модели критерию эффективности информационной безопасности.

Проверить соответствие математической модели критерию эффективности информационной безопасности P_2>=0.8. В случае несоответствия, вернуться к пункту работ, чтобы увеличить интенсивности процессов управления. Расчет математической модели выполним с помощью программного кода, написанного на Piton (приложение 1).

Результат выполнения программного кода представлен на рисунке №10.

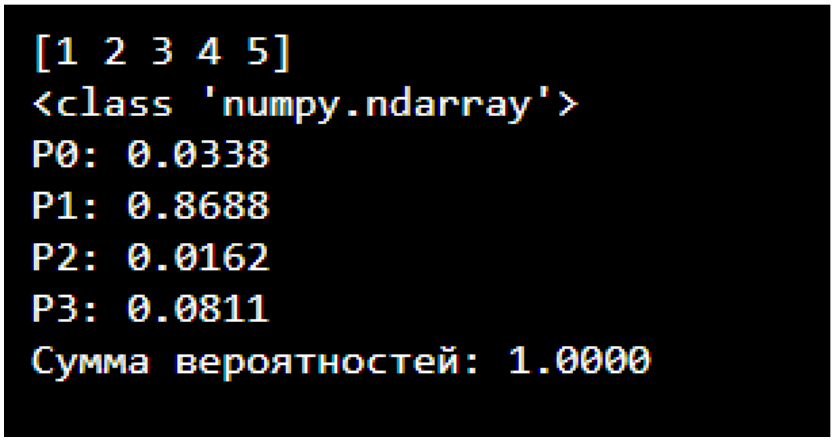


Рисунок №10 Результат вычисления

Получившееся значение (P2 = 0.8688) соответствует критерию эффективности математической модели информационной безопасности $P_Ц$>=0.80.

Выводы по главе 2

Разработанная в главе 2 аналитико-динамическая модель представляет собой эффективный инструмент для системного управления ИБ в образовательной организации.

Системный подход к моделированию. Модель может представляет собой а целостный управленческий цикл. Она начинается с проактивного контроля и идентификации угроз через анализ событий (IDS/IPS, сканирование уязвимостей, аудит), продолжается оперативными процедурами нейтрализации инцидентов и завершается процессами постоянного функционирования, направленными на поддержание системы в безопасном состоянии. Это обеспечивает непрерывность и замкнутость процесса управления ИБ [23, 27]..

Детализация и количественная оценка. Для каждого процесса построены сетевые графики (ПЕРТ), включающие перечни событий и работ с указанием их длительности и логической последовательности. Проведен расчет временных параметров: ранних и поздних сроков свершения событий, резервов времени. Это позволило:

выявить критический путь — последовательность работ, определяющую общую длительность процесса, не имеющих резервов времени (например, работы А0-1, А1-4, А4-5, А5-8, А8-13, А13-14 в модели контроля).

определить «узкие места» и работы с большими резервами, что дает возможность оптимизировать распределение ресурсов и повысить эффективность процессов [24, 28].

Целевая направленность процессов.

Контроль: Основная цель — минимизация времени обнаружения ($t_{обн}$) угроз. Модель акцентирует внимание на ключевых индикаторах компрометации для каждого вектора (физический износ, уязвимости ПО, аномалии в поведении пользователей).

Нейтрализация: Направлена на минимизацию ущерба и времени восстановления. Предложены конкретные меры реагирования, от изоляции угрозы до устранения ее причины и восстановления сервисов.

Функционирование: Ориентирована на максимизацию времени безотказной работы ($t_{пр}$) и профилактику инцидентов через плановое обслуживание, управление жизненным циклом, обучение персонала и настройку превентивных политик (принцип наименьших привилегий, DLP).

4. Верификация адекватности модели. Математическая проверка модели по критерию эффективности (вероятность нахождения системы в целевом состоянии P2 >= 0.8) с использованием программной реализации дала положительный результат: P2 = 0.8688. Это подтверждает, что разработанная модель с заданными интенсивностями процессов управления способна обеспечить требуемый уровень надежности и безопасности информационной системы образовательной организации [27].

Процессная модель является эффективным инструментом для системного управления ИБ. Модель соответствует установленному критерию эффективности и может служить основой для построения реальной системы безопасности или аудита существующей. На основе 2 главы необходимо построить методику достижения времени идентификации, что позволит составить четкий, алгоритмизированный и количественно обоснованный план

действий для своевременного выявления, реагирования на угрозы и поддержания устойчивого функционирования ИТ-инфраструктуры.

ГЛАВА 3. МЕТОДИКА ПРИМЕНЕНИЯ АНАЛИТИКО-ДИНАМИЧЕСКОЙ МОДЕЛИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1. Алгоритм внедрения и использования модели

Разработанная в главе 2 аналитико-динамическая модель предоставляет не только теоретическую основу, но и практический инструментарий для повышения эффективности системы обеспечения информационной безопасности (ИБ) образовательной организации. На основе концептуальной модели можно построить систему ИБ. Используя модель из 2 главы, можно ее доработать под нужные параметры. Данная глава описывает методику внедрения и использования модели, позволяющую перейти от формального описания процессов к их оперативному управлению и постоянному совершенствованию. Методика направлена на достижение ключевой цели — минимизацию временных лагов между возникновением угрозы и её нейтрализацией, что напрямую повышает устойчивость информационной среды.

Применение моделей представляет собой циклический процесс, состоящий из последовательных этапов, адаптированных под специфику образовательного учреждения (наличие учебных классов, научных баз данных, персональных данных учащихся и сотрудников).

Этап 1. Инициализация и настройка (Соответствует состоянию «Функционирование»).

Цель: Приведение существующей системы ИБ в соответствие с параметрами модели, построенной на основе концептуальной модели, создание стартовых условий для её работы.

Необходимы следующие действия п

1. Аудит и инвентаризация: провести детальный аудит всей ИТ-инфраструктуры (аппаратное обеспечение, ПО, сеть, ресурсы) и процессов ИБ.

Результаты занести в реестры, соотнести с элементами моделей из разделов 2.1-2.4.

2. Назначение ответственных: определить и формально закрепить за сотрудниками обязанности, соответствующие вершинам и работам сетевых графиков (например, ответственный за мониторинг IDS/IPS – событие `a4` в модели контроля, специалист по реагированию – работы `A0-1`, `A1-4` в модели нейтрализации).

3. Калибровка временных параметров: на основе данных аудита и исторических инцидентов (если есть) установить реальные базовые значения для ключевых параметров:

`$t_{пр}$` (среднее время проявления проблемы) – по данным о частоте сбоев оборудования и ПО.

`$t_{обн}$` (среднее время обнаружения) – по данным журналов SIEM и времени реакции SOC.

`$t_{нейтр}$` (среднее время нейтрализации) – по данным об устранении прошлых инцидентов.

4. Настройка инструментов: Обеспечить интеграцию систем мониторинга (SIEM, IDS/IPS, DLP, системы контроля доступа) для автоматической фиксации событий, соответствующих вершинам графов контроля (`a1` – аномальная активность, `a2` – результат сканирования и т.д.).

Этап 2. Оперативный мониторинг и идентификация (Соответствует процессам P2 и P3, модель «Контроль»).

Цель: Непрерывное отслеживание состояния системы и своевременное обнаружение отклонений от нормального функционирования.

Действия:

1. Работа по сценариям: Использовать сетевой график контроля (Рисунок 7, Таблицы 7-8) как карту возможных инцидентов. Например, при срабатывании IDS (событие `a4`) автоматически инициируется процесс корреляции событий (работа `A4-5`).

2. Контроль критического пути: Особое внимание уделять работам, лежащим на критическом пути модели контроля (например, `A0-1` → `A1-4` → `A4-5` → `A5-8` → `A8-13` → `A13-14`). Задержки на этих этапах напрямую увеличивают общее время реагирования (`t_обн`). Мониторинг их длительности должен быть приоритетным.

3. Использование резервов: Работы с большим полным резервом времени (например, `$R_П(2,6)=8$` в Таблице 12) указывают на возможности для перераспределения ресурсов в пользу критических задач в момент пиковой нагрузки.

Этап 3. Реагирование и нейтрализация (Соответствует процессу Р4, модель «Нейтрализация»).

Цель: Оперативное и эффективное устранение выявленной угрозы, минимизация ущерба.

Действия:

1. Активация плана реагирования: Зафиксированный инцидент (событие `a14` модели контроля) служит триггером для запуска сетевого графика нейтрализации (Рисунок 8). Ответственный переходит к выполнению работы `A0-1` (Изоляция).

2. Следование регламентированной последовательности: Использовать граф нейтрализации как пошаговый чек-лист. Например, после изоляции (`A0-1`) следует блокировка активности (`A1-4`), затем применение правил (`A4-8`) и т.д. Это исключает хаотичные действия и гарантирует учет всех необходимых мер.

3. Управление по критическому пути: Анализ графика нейтрализации (Таблицы 15-17) позволяет заранее выделить этапы, не имеющие резерва (например, `A0-3` → `A3-7` → `A7-10`), и обеспечить их максимально быстрое выполнение, выделив дополнительные ресурсы.

Этап 4. Восстановление и анализ (Связывает модели «Нейтрализация» и «Функционирование»).

Цель: Возврат системы в штатный режим работы и извлечение уроков для повышения устойчивости.

Действия:

1. Верификация восстановления. Завершающее событие модели нейтрализации (`a14` – Устранение) должно сопровождаться проверкой критериев возврата в нормальное состояние (соответствие показателей модели «Функционирования»).

2. Анализ временных параметров. По итогам инцидента фиксируются фактические значения `t_обн_факт` и `t_нейтр_факт`. Они сравниваются с базовыми и плановыми показателями.

3. Корректировка моделей: на основе анализа вносятся изменения

Если модель угроз выявлен новый вектор атаки, он добавляется в граф (Рисунок 6) и таблицы угроз.

В модели контроля и нейтрализации. Если какая-то работа заняла аномально много времени, анализируются причины и вносятся корректировки в регламенты, назначаются дополнительные ресурсы или проводится обучение персонала. Это эквивалентно увеличению интенсивности соответствующих процессов управления в математической модели.

В модель функционирования: Выявленные root-причины инцидента приводят к усилению превентивных мер (например, более частая установка обновлений `A0-1`, ужесточение политик аудита `A6-9`).

Планирование и распределение ресурсов: Сетевые графики с рассчитанными временами работ служат основой для составления графиков дежурств SOC, планирования профилактических работ (обновления, аудиты) и формирования бюджета на ИБ (закупка инструментов мониторинга, обучение).

Обучение и тренировки персонала: Модели, особенно графики нейтрализации, являются идеальной основой для разработки сценариев учебных тревог (CTF-упражнений, table-top exercises). Сотрудники отрабатывают

действия в рамках четкого алгоритма, что снижает время реального реагирования.

Взаимодействие с подразделениями: Модель наглядно демонстрирует взаимосвязь между техническими службами (ИТ-отдел), службой безопасности, администрацией и учебными подразделениями. Например, событие `a13` в модели контроля («Массовые инциденты от пользователей») требует четкого регламента взаимодействия с деканатами и преподавателями для информирования и сбора данных.

Документирование и отчетность: Все этапы работы по модели автоматически формируют основу для отчетности. Логи событий, время выполнения работ, переходы между состояниями фиксируются и могут быть использованы для отчетов перед руководством или регуляторами, демонстрируя зрелость процессов ИБ.

3.3. Практический пример применения методики

Ситуация: В университете зафиксирована массовая жалоба пользователей на недоступность учебного портала (событие `a13` модели контроля).

Действия по методике:

1. Идентификация (Этап 2): SOC, используя граф контроля, немедленно инициирует корреляцию (`A8-13`). Анализ показывает срабатывание IDS на сетевом оборудовании (`a4`) и аномальное потребление ресурсов (`a3`). Критический путь активирован.

2. Нейтрализация (Этап 3) Объявляется инцидент. Запускается граф нейтрализации. Ответственный:

`A0-3` Немедленно блокирует входящий трафик к серверу портала (прерывание атаки).

`A3-6` Анализирует логи, выявляет DDoS-атаку с внутренних зараженных рабочих станций.

Параллельно `A3-7` Блокирует скомпрометированные учетные записи студентов, с чьих устройств идет атака.

`A6-10` / `A7-10` Настраивает правила фильтрации на маршрутизаторе и обновляет сигнатуры антивируса.

`A10-12` Перенастраивает балансировщик нагрузки для восстановления доступности.

3. Восстановление и анализ (Этап 4):

`A12-14` После стабилизации сервис возвращен в работу.

Фиксируется: `$t_{обн}$_факт = 5 мин`, `$t_{нейтр}$_факт = 25 мин`.

Анализ: Обнаружено, что заражение рабочих станций произошло из-за несанкционированного ПО, установленного студентами (уязвимость ресурса). Работа `A9-13` модели контроля («Реализация рисков из-за слабого контроля») имела большой резерв, но не предотвратила инцидент.

Корректировка моделей:

В модель функционирования вносится усиление работы `A9-12` («Инвентаризация и контроль соответствия конечных точек политикам») – внедряется система централизованного управления endpoint security.

В модель нейтрализации уточняется сценарий `A3-7` для быстрого взаимодействия с деканатом по блокировке сетевого доступа нарушителям.

3.4. Критерии эффективности применения методики

Успешность внедрения методики оценивается по динамике следующих показателей:

- снижение среднего времени взаимодействия с угрозами: устойчивое сокращение фактических значений `$t_{обн}$` и `$t_{нейтр}$` по сравнению с базовыми.

- рост вероятности целевого состояния: контрольное значение `P2` (рассчитанное по актуальным интенсивностям) должно оставаться не ниже 0.8 и стремиться к росту.

- Сокращение количества инцидентов: уменьшение числа успешных атак за счет улучшения процессов функционирования (профилактики).

- Увеличение полноты охвата: рост процента инцидентов, отраженных в моделях и обработанных по регламентам.

- Оперативность корректировок: сокращение времени между анализом инцидента и внесением улучшающих изменений в модели и регламенты.

Выводы по главе 3

Предложенная методика переводит теоретическую аналитико-динамическую модель в плоскость практического управления. Она обеспечивает структурированный, алгоритмизированный подход к обеспечению ИБ, что особенно важно для образовательных организаций с их ограниченными ресурсами и высокими требованиями к защите данных. Цикличность методики (функционирование → контроль → нейтрализация → анализ → корректировка функционирования) гарантирует постоянное развитие системы безопасности, её адаптацию к новым угрозам и соответствие критерию эффективности. Использование сетевых графиков в качестве основы для регламентов, тренировок и отчетности делает процессы ИБ прозрачными, измеримыми и управляемыми, что в конечном итоге способствует созданию устойчивой и безопасной информационной среды для образовательного процесса.

ГЛАВА 4. НАУЧНО-ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ МЕТОДИКИ ПОСТРОЕНИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

4.1. Обоснование научного фундамента методологии

Представленные в предыдущих главах модели управления ИБ вуза требует всестороннего обоснования для подтверждения её научной ценности и практической значимости. Цель данной главы — дать комплексный ответ на три критических вопроса, определяющих жизнеспособность любой управленческой методики: на чем она основана, в чем её новизна и эффективность, и как она может быть реализована с учетом экономических ограничений вуза. Особое внимание уделяется экономическому аспекту, так как именно ресурсные ограничения, отмеченные в работах [12, 27], являются ключевым барьером для построения эффективных систем ИБ в образовании.

Методика построена на синтезе проверенных научных и прикладных подходов, адаптированных к специфике образовательной среды.

Общий подход к описанию системы ИБ вуза как целостного объекта с состояниями, переходами и управляющими воздействиями базируется на принципах системного анализа [23, 25]. В частности, использованная в Главе 2 аналитико-динамическая модель, описывающая поведение системы через состояния P1-P4, является развитием методологии моделирования управленческих решений в социально-экономических системах, предложенной в [27]. Это обеспечивает системный взгляд на ИБ, выходящий за рамки чисто технических мер.

Процессно-ориентированный подход и управление рисками. Декомпозиция деятельности службы ИБ на формализованные процессы (графы) и их привязка к состояниям системы прямо вытекает из процессного подхода к управлению ИБ, описанного в стандартах серии ISO/IEC 27000 [7, 13] и трудах по управлению рисками [1, 16]. Такой подход позволяет перейти от разрозненных мероприятий к управляемым и воспроизводимым бизнес-процессам.

Интеграция требований регуляторов и лучших практик. Модель сознательно интегрирует требования ключевых для РФ документов: Федеральных законов № 149-ФЗ и № 152-ФЗ [6, 20], Приказа ФСТЭК № 21 [22], а также международного стандарта ISO/IEC 27001 [7]. Это обеспечивает правовую и нормативную обоснованность методики, делая её не теоретической конструкцией, а практическим инструментом для достижения соответствия.

Учет человеческого фактора как системного элемента. Выделение работы с пользователями (сотрудниками и студентами) в отдельный управляемый процесс основано на понимании, что культура ИБ является критическим фактором безопасности [10]. Это позволяет перенести фокус с технической защиты на формирование устойчивого безопасного поведения, что особенно актуально в открытой академической среде.

Каждый элемент методики имеет прямые отсылки к устоявшимся теориям, стандартам и практикам в области ИБ и управления. Их объединение создает прочный методологический фундамент, обеспечивающий системность,

соответствие нормам и ориентацию на ключевые риски образовательного учреждения.

4.2. Вопрос новизны и эффективности: синтез как инновационное решение

Новизна предлагаемой методики заключается не в изобретении новых принципов, а в их целенаправленном синтезе для решения поставленных задач в ИБ вуза.

1. От статического соответствия к динамическому управлению. В отличие от классических подходов, часто фокусирующихся на достижении формального соответствия стандартам («чек-листовый» подход) [1, 11], построенная модель делает акцент на динамике. Она описывает не статичное состояние защищенности, а непрерывный цикл функционирования, контроля и адаптации (P1→P2→P3→P4→P1). Это напрямую отвечает на критику о неэффективности статических мер в условиях эволюции угроз [12].

2. Мост между стратегической моделью и тактическими регламентами. Методика преодолевает разрыв между абстрактными политиками ИБ [5, 17] и повседневной работой администраторов. Аналитическая модель (Глава 2) задает стратегические цели и количественные критерии (например, целевой уровень вероятности состояния P2), а методика построенная в главе 3 предоставляет инструкции по достижению задач, оптимизируя время и усилия персонала.

3. Инструмент для обоснования управленческих решений и инвестиций. Введение количественного критерия эффективности (поддержание вероятности P2 на уровне ≥ 0.8) и использование аппарата вероятностного моделирования позволяет проводить сценарный анализ «что-если». Руководство вуза может оценить, как увеличение частоты контроля (требующее затрат) или ускорение процедур нейтрализации (требующее пересмотра процессов или автоматизации) повлияет на общий уровень безопасности. Это переводит дискуссию о финансировании ИБ из плоскости субъективных мнений в плоскость обоснованных расчетов и управленческих KPI [27].

Синтез создает эмерджентный эффект практической применимости. Методика предлагает не просто ещё один framework, а связанный управленческий контур «модель-процесс-критерий», который позволяет целенаправленно использовать ограниченные ресурсы для максимального повышения устойчивости системы ИБ.

4.3. Практическая применяемость и экономическая целесообразность построенной методики

Научная обоснованность и новизна должны подтверждаться реализуемостью и экономическим смыслом внедрения в условиях вуза с ограниченным бюджетом.

Поэтапное внедрение и минимизация первоначальных затрат. Ключевое экономическое преимущество методики — её модульность и поэтапность. Вуз не обязан внедрять всё и сразу. Можно начать с моделирования и оптимизации одного-двух наиболее болезненных процессов (например, реагирование на инциденты с утечкой ПДн [3, 20] или восстановление после сбоя). Это требует не капитальных вложений в дорогое ПО, а в первую очередь интеллектуальных затрат на аудит и формализацию существующих процедур силами штатных специалистов, возможно, с привлечением методологической поддержки. Такой подход резко снижает барьер входа для внедрения.

Оптимизация операционных расходов (OPEX) через процессный анализ. Основная экономия методики проявляется в повседневной операционной деятельности. Применение PERT-анализа для регламентов ИБ позволяет:

Сократить время реагирования на инциденты за счет выявления и оптимизации «узких мест» в критическом пути. Это напрямую снижает потенциальный ущерб от простоев учебных порталов или утечек данных, что имеет прямую финансовую и репутационную выгоду.

Повысить эффективность работы специалистов ИБ. Четкие, оптимизированные регламенты избавляют от хаотичных действий, уменьшают время на согласования и рутину. Высвобожденный ресурс можно направить на более стратегические задачи, такие как анализ угроз или обучение пользователей.

Целесообразно обосновать автоматизацию. PERT-граф наглядно показывает, автоматизация каких именно рутинных операций (например, сбор доказательств по инциденту) даст максимальный прирост скорости и высвобождение человеческих ресурсов. Это позволяет приоритизировать ИТ-инвестиции [28].

Качественные экономические выгоды и управление рисками.

Снижение репутационных и регуляторных рисков. Стабильная и документированная система ИБ минимизирует вероятность крупных инцидентов, способных нанести урон репутации вуза и повлечь штрафы от

регуляторов [6, 20, 22]. Это защита от потенциально больших финансовых потерь.

Создание нематериального актива. Формализованные модели процессов и регламенты становятся корпоративным знанием, снижая зависимость от конкретных сотрудников и облегчая onboarding новых специалистов.

Повышение зрелости управления. Подход способствует переходу от реактивной к проактивной модели управления ИБ, что в долгосрочной перспективе является самым экономически эффективным сценарием [1, 16].

4. Верификация и валидация применимости. Работоспособность методики подтверждается на нескольких уровнях:

Теоретическая верификация: Расчет стационарных вероятностей состояний системы (как в Главе 2) использует проверенный математический аппарат [23, 27], подтверждая внутреннюю непротиворечивость модели.

Прагматическая валидация: Методика напрямую опирается на требования актуальных российских и международных стандартов [7, 22], что подтверждает её адекватность лучшим отраслевым практикам.

Контекстуальная валидация: Фокус на оптимизацию процессов, а не на дорогостоящие закупки, и учет специфики образовательной среды [3, 10, 12] доказывают, что методика создана для решения реальных проблем вузов.

Методика является экономически эффективной стратегией. Она смещает фокус с капиталоёмких «точечных» закупок средств защиты на инвестиции в оптимизацию процессов и человеческий капитал. Это позволяет вузу добиваться измеримого прогресса в зрелости ИБ, распределяя часто ограниченные финансовые ресурсы наиболее рациональным и обоснованным образом.

Таким образом, представленная аналитико-динамическая методика получила комплексное обоснование:

научный фундамент: Она опирается на солидную базу теорий системного анализа, управления рисками, процессного подхода и актуальных нормативных требований.

инновационная сущность: Её новизна в эффективном синтезе этих компонентов в целостный управленческий контур, обеспечивающий динамичность, измеримость и целевое использование ресурсов.

практическая и экономическая целесообразность: методика предлагает реалистичный, поэтапный путь внедрения, ведущий к оптимизации

операционных расходов, снижению рисков и повышению общей эффективности системы ИБ вуза, что прямо отвечает на вызовы, сформулированные в начале исследования.

Вывод по работе.

В дипломной работе достигнута поставленная цель — на основе анализа угроз и нормативной базы создана комплексная модель безопасности информации образовательной организации. На ее основе разработанна аналитико-математическая модель и практическая методика её применения. Работа представляют собой научно обоснованный, экономически целесообразный и практико-ориентированный инструмент. Он позволяет руководству и службе ИБ вуза системно управлять безопасностью, целенаправленно использовать ресурсы для минимизации рисков и обеспечивать устойчивое функционирование информационной среды в интересах учебного и научного процессов. Работа вносит вклад в решение актуальной проблемы повышения зрелости систем ИБ в сфере высшего образования. Разработанная методика сложна для построения системы информационной безопасности и требует доработок, однако ее не сложно интегрировать в уже существующую систему, что качественно улучшит ее показатели для данных нормативных актов и угроз.

Список использованных источников

1. Петренко, С. А. Управление информационными рисками: учебное пособие / С. А. Петренко. – Москва: Горячая линия – Телеком, 2020. – 254 с.
2. Галатенко, В. А. Основы информационной безопасности: учебник для вузов / В. А. Галатенко. – 4-е изд., испр. – Москва: Интернет-Университет Информационных Технологий, 2019. – 480 с.
3. Рогозин, А. В. Защита персональных данных в образовательных учреждениях: практическое руководство / А. В. Рогозин, М. М. Кондрашин. – Санкт-Петербург: БХВ-Петербург, 2021. – 192 с.
4. Галатенко В.А. Основы информационной безопасности: учеб. пособие. М.: Интернет-Университет Информационных Технологий, 2015. – 264 с.
5. Петренко С.А., Курбатов В.А. Политики информационной безопасности. М.: Компания АйТи; ДМК Пресс, 2006. – 400 с.
6. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.02.2021) «Об информации, информационных технологиях и о защите информации». – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 20.03.2025).
7. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
8. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД «ФОРУМ»: ИНФРА-М, 2018. – 416 с.
9. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности: учеб. пособие. М.: Радио и связь, 2000. – 192 с.
10. Скиба В.И., Шестопалова И.В. Формирование культуры информационной безопасности в образовательной организации // Информационная безопасность регионов. 2020. № 2(35). С. 85–90.
11. Черников Б.В. Безопасность информационных систем: учебник. М.: КноРус, 2021. – 324 с.
12. Аверченков В.И., Гамолина О.В., Рытов М.Ю. Актуальные проблемы информационной безопасности в системе высшего образования // Вестник Брянского государственного технического университета. 2019. № 3(76). С. 32–40.

13. ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary. – 4th ed. – 2018.

14. Модель информационной безопасности // Справочник. – URL: https://spravochnick.ru/informatika/model_informacionnoy_bezopasnosti/ (дата обращения: 20.10.2023).

15. Kindervag, J. Build Security Into Your Network's DNA: The Zero Trust Network Architecture // Forrester Research. – 2010.

16. Петренко, С. А. Управление информационными рисками: учебное пособие / С. А. Петренко, А. А. Курбатов. – М.: Горячая линия – Телеком, 2018. – 280 с.

17. Информационная безопасность и защита информации: учебное пособие / под ред. Л. Г. Осовецкого. – СПб.: Лань, 2019. – 412 с.

18. Баричев, С. Г. Основы современной криптографии и стеганографии / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. – М.: Горячая линия – Телеком, 2015. – 236 с.

19. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 24.02.2024) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3448.

20. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) // Собрание законодательства РФ. – 2006. – № 31 (1 ч.). – Ст. 3451.

21. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 05.12.2022) // Собрание законодательства РФ. – 2002. – № 1 (ч. 1). – Ст. 3.

22. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ ФСТЭК России от 18.02.2013 № 21 (ред. от 16.11.2020) // Бюллетень нормативных актов федеральных органов исполнительной власти. – 2013. – № 34.

23. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (методология, методы). СПБ: изд-во СПБГПУ, 2007.

24. Цветков В.Я., Матчин В.Т. Агрегирование информационных моделей // Славянский форум. 2014. №2(6). С. 77-81.

25. Гуд Г.Х., Макол Р.Э. Системотехника. М.: Советское радио, 1962. 384 с.

26. Бурлов В.Г., Попов Н.Н., Гарсия Эскалона Х.А. Управление процессом применения космической геоинформационной системы в интересах обеспечения экологической безопасности региона // Ученые записки РГГМУ. 2018. №50. С. 45-52.

27. Бурлов В.Г., Грачев М.И. Аналитическо-динамическая модель управленческого решения в социально-экономических системах на примере руководителя учебного заведения высшего образования // T-Comm: Телекоммуникации и транспорт. 2019. Т. 13. №10. С. 27-34.

28. Бурлов В.Г. Методы моделирования в экономике. Часть 1. СПБ: изд-во СПбГПУ, 2007. 330 с.

29. DDoS-атаки на вузы: как подготовиться и защититься в 2024

https://ddos-guard.ru/blog/ddos-ataki-na-uchebnie-zavedeniya

Приложение 1

```
  import numpy as np

arr = np.array([1, 2, 3, 4, 5])

print(arr)

print(type(arr))
import numpy as np
def solve_markov_chain(lambda01, lambda02, lambda10, lambda13, lambda23, lambda30, lambda31):
  A = np.array([
      [-(lambda01 + lambda02), lambda10, 0, lambda30],
      [lambda01, -(lambda10 + lambda13), 0, lambda31],
      [lambda02, 0, -lambda23, 0],
      [1, 1, 1, 1]
  ], dtype=float)
  det_A = np.linalg.det(A)
  if abs(det_A) < 1e-10:
    print("Система не имеет единственного решения (определитель близок к 0).")
    return None
  A_P0 = np.array(A)
  A_P0[:, 0] = [0, 0, 0, 1]
  A_P1 = np.array(A)
  A_P1[:, 1] = [0, 0, 0, 1]
  A_P2 = np.array(A)
  A_P2[:, 2] = [0, 0, 0, 1]
  A_P3 = np.array(A)
  A_P3[:, 3] = [0, 0, 0, 1]

  det_P0 = np.linalg.det(A_P0)
  det_P1 = np.linalg.det(A_P1)
  det_P2 = np.linalg.det(A_P2)
  det_P3 = np.linalg.det(A_P3)
  P0 = det_P0 / det_A
  P1 = det_P1 / det_A
  P2 = det_P2 / det_A
  P3 = det_P3 / det_A
  return P0, P1, P2, P3
lambda01 = 10.0
lambda02 = 8.0
lambda10 = 2.5
lambda13 = 8.0
lambda23 = 66.0
lambda30 = 6.0
lambda31 = 83.0
result = solve_markov_chain(lambda01, lambda02, lambda10, lambda13, lambda23, lambda30,
lambda31)
if result:
  P0, P1, P2, P3 = result
  print(f"P0: {P0:.4f}")
  print(f"P1: {P1:.4f}")
  print(f"P2: {P2:.4f}")
  print(f"P3: {P3:.4f}")
  print(f"Сумма вероятностей: {P0 + P1 + P2 + P3:.4f}")
```