МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Методическое обеспечение процесса выявления инцидентов в работе комплексных сетей систем безопасности образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения заочная

Проверка на объем заимствований:
73,99 % авторского текста
Работа рекомендована к защите
«26» 01 2026 г.
Доцент кафедры АТИТ и МОТД
_____ Гафарова Е.А.
Заведующий кафедрой АТИТ и МОТД
Рудаев В.В

Выполнила:
Студентка группы ЗФ-309-210-2-1,
Шаталова Анна Александровна

Научный руководитель:
доцент кафедры, к.п.н.,
Гафарова Елена Аркадьевна

Челябинск
2026

Содержание

ВВЕДЕНИЕ

Актуальность

В современном мире обеспечение безопасности в образовательных организациях становится всё более значимой задачей. Это обусловлено несколькими факторами. Во-первых, образовательные учреждения обрабатывают и хранят большие объёмы персональных данных обучающихся и персонала, что делает их привлекательными целями для киберпреступников [60]. Во-вторых, растущее использование цифровых технологий в образовании увеличивает риск инцидентов, связанных с нарушением информационной безопасности. В-третьих, образовательные организации должны соответствовать строгим нормативным требованиям по защите данных и обеспечению безопасности [48].

Комплексные сети систем безопасности играют ключевую роль в защите образовательных учреждений. Они включают в себя различные компоненты, такие как датчики, контроллеры, серверы и программное обеспечение, которые работают вместе для мониторинга, анализа и реагирования на инциденты [10, 35]. Однако эффективность этих систем во многом зависит от качества методического обеспечения процесса выявления инцидентов [47].

В условиях цифровизации образовательные организации сталкиваются с резким ростом киберугроз: хакерскими атаками, распространением вредоносного ПО, фишингом. Это создаёт риски утечки конфиденциальных данных (персональных сведений студентов и сотрудников, интеллектуальной собственности) и срыва учебного процесса [60, 61].

Статистика подтверждает остроту проблемы: по данным «Информзащиты» (2024 г.):

— 74 % образовательных учреждений столкнулись с инцидентами информационной безопасности;

— 60 % учреждений подверглись сливу персональных данных;

— 46 % — фишинговым атакам;

— 35 % — атакам с применением вредоносного ПО [67].

При этом высшие учебные заведения наиболее уязвимы (57 % атак), за ними следуют учреждения среднего профессионального образования (23 %) и школы (20 %) [67].

Обеспечение кибербезопасности становится приоритетной задачей для защиты данных и бесперебойной работы образовательных организаций.

Современная парадигма развития образования неразрывно связана с цифровой трансформацией: образовательные организации масштабируют использование цифровых технологий (ЦТ), что влечёт интенсификацию информационных потоков и усложнение ИТ-инфраструктуры [36, 51]. Параллельно с этим фиксируется эскалация киберугроз: злоумышленники целенаправленно адаптируют передовые технологии для атак на образовательные учреждения, эксплуатируя уязвимости комплексных сетей систем безопасности [8, 15].

Анализ текущей ситуации выявил следующие существенные пробелы:

1) существующие методы выявления инцидентов в комплексных сетях систем безопасности не в полной мере учитывают специфику распределённых и гетерогенных ИТ-сред образовательных организаций.

2) отсутствуют стандартизированные методические подходы к анализу и реагированию на инциденты в комплексных сетях систем безопасности, что приводит к фрагментарности защитных мер и замедлению реакции на угрозы.

Данные обстоятельства актуализируют необходимость разработки специализированного методического обеспечения для образовательных учреждений. В связи с этим тема исследования сформулирована следующим образом: «Методическое обеспечение процесса выявления

инцидентов в работе комплексных сетей систем безопасности образовательной организации».

Тема находится на стыке нескольких научных дисциплин, что подчёркивает её междисциплинарный характер и комплексность подхода к решению проблемы обеспечения безопасности в образовательных учреждениях. Для полноценного исследования необходимы знания и подходы «Информационной безопасности» (в аспекте понимание угроз, уязвимостей и рисков, связанных с обработкой и хранением данных в образовательных организациях) [6, 21], «Кибербезопасности» (для адаптации инструментов и методов для обнаружения и предотвращения кибератак) [26, 28], «Системный анализ и управление» (для оценки структуры и функций комплексных сетей систем безопасности, выявления слабых мест и разработки эффективных методов управления рисками) [2, 42], «Педагогика и образование» (для адаптации методов обеспечения безопасности под конкретные условия и потребности образовательных учреждений) [12, 37], «Прикладная математика и статистика» (для анализа данных о выявленных инцидентах, оценки их частоты и вероятности, а также прогнозирования возможных будущих инцидентов) [5, 46], «Менеджмент рисков» (для идентификации потенциальных угроз, оценки их вероятности и последствий, а также разработки мер по их минимизации) [1, 51], «Технологии защиты информации» (для изучения современных технологий шифрования, аутентификации, контроля доступа и других методов защиты данных) [4, 29], «Право и нормативные требования» (для обеспечения соответствия систем безопасности требованиям законодательства и нормативных документов) [9, 60, 61].

Таким образом, тема магистерской диссертации объединяет различные области знаний, что позволяет разработать комплексный подход к обеспечению безопасности в образовательных организациях и эффективно решать задачи по выявлению и предотвращению инцидентов в работе комплексных сетей систем безопасности.

Объектом исследования являются комплексные сети систем безопасности образовательных организаций.

Предметом исследования являются процессы выявления инцидентов в комплексных сетях систем безопасности образовательных организаций.

Целью данной магистерской диссертации является разработка методического обеспечения для эффективного выявления инцидентов в работе комплексных сетей систем безопасности в образовательной организации.

Гипотеза исследования заключается в предположении, что применение разработанного методического подхода позволит повысить эффективность выявления инцидентов и оперативно реагировать на них, что в свою очередь повысит общий уровень безопасности в образовательных организациях.

В соответствии с объектом, предметом и целью исследования были поставлены следующие задачи:

1) сформулировать уточненное определение понятий «инцидент» и «безопасность», выделить виды безопасности, определить структуру и функции комплексных сетей систем безопасности, определить классификацию инцидентов;

2) провести анализ существующих методов выявления инцидентов в системах безопасности (на базе исследования);

3) усовершенствовать существующие методы, разработать / актуализировать алгоритм выявления инцидентов, включающий последовательность шагов для сбора, анализа и классификации данных с учётом специфики образовательных организаций (на базе исследования);

4) оценить эффективность предложенного методического обеспечения на основе полученных данных путем экспертной оценки.

Теоретико-методологической основой исследования являются работы отечественных и зарубежных учёных в области информационной

безопасности, управления рисками и системного анализа. Задача обнаружения инцидентов является комплексной и имеет множество решений, которые зависят от конкретной области применения. Эта проблема в разных аспектах рассматривается в работах В. А. Гладцына [13], А. А. Грушо [21], В. В. Меньших [42], А. А. Шелупанова [6], П. Д. Зегжды [26], И. В. Бондаря [7, 8], В. В. Золотарёва [27], А. М. Попова [46], Л. Глизенте, Р. Хоури, Ш. К. Чина, Kim Zetter и других отечественных и зарубежных учёных.

Для решения поставленных задач и проверки гипотезы используются следующие **методы исследования**: анализ научной литературы и нормативных документов; сравнительный анализ существующих подходов к выявлению инцидентов; статистические методы для анализа данных о выявленных инцидентах; экспертная оценка.

База исследования: государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный колледж».

Научная новизна исследования заключается в разработке нового методического подхода к выявлению инцидентов в работе комплексных сетей систем безопасности образовательной организации, который учитывает специфику образовательных учреждений и позволяет повысить эффективность процесса выявления инцидентов.

Теоретическая значимость исследования состоит в расширении научных знаний в области обеспечения безопасности образовательных организаций и разработке новых методов и алгоритмов выявления инцидентов.

Практическая значимость: результаты данного исследования могут быть использованы для улучшения процесса выявления инцидентов в работе комплексных сетей систем безопасности в образовательных организациях. Предложенные методы и алгоритмы могут помочь повысить

эффективность систем безопасности и снизить риски, связанные с нарушениями безопасности.

Основные этапы исследования:

1) на первом этапе формулировались тема исследования и план диссертации; выполнялся сбор информации по вопросу исследования из различных источников, осуществлялась формулировка гипотезы, постановка цели и задач;

2) на втором этапе проводилась комплексная работа, включающая в себя: изучение научной и технической литературы, отбор необходимых источников информации, анализ существующих методов выявления инцидентов, публикация научных статей по теме исследования;

3) на третьем этапе осуществлялся анализ методов выявления инцидентов на базе исследования, разработка нового методического подхода и алгоритма выявления инцидентов в профессиональной образовательной организации на базе исследования, оценка эффективности предложенного методического обеспечения путем экспертной оценки, а также текстовое оформление материалов исследования, формулировка выводов.

Структура диссертации. Магистерская диссертация включает введение, три главы, выводы по главам, заключение, список использованных источников, приложения.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

1.1 Понятие и виды безопасности в образовательных организациях

Безопасность в образовательных организациях — это комплекс мер, направленных на защиту жизни и здоровья участников образовательного процесса, а также на сохранение материальных и информационных ресурсов [33, 41]. Это многогранный процесс, требующий системного подхода и учёта различных аспектов, которые могут повлиять на нормальное функционирование образовательной среды [2, 42]. Безопасность в образовательных организациях включает в себя несколько видов, каждый из которых имеет свои особенности и требует специфических подходов к обеспечению [10, 35].

1. Физическая безопасность — обеспечение защиты зданий, сооружений и территории организации от несанкционированного доступа, а также предотвращение возможных террористических угроз [17, 38]. Физическая безопасность включает в себя следующие элементы:

— установка систем видеонаблюдения для мониторинга территории и помещений [10, 33];

— внедрение систем контроля доступа, ограничивающих вход в здание посторонним лицам [38, 51];

— использование охранной сигнализации для своевременного реагирования на попытки проникновения [10, 17];

— регулярное патрулирование территории охранными службами [33, 41].

2. Информационная безопасность — защита информации, обрабатываемой и хранящейся в информационных системах организации, от несанкционированного доступа, использования, раскрытия, изменения

или уничтожения [6, 21]. Важными аспектами информационной безопасности являются:

— защита персональных данных обучающихся и сотрудников, которые хранятся в информационных системах [43, 60];

— обеспечение бесперебойной работы информационных систем, необходимых для образовательного процесса [28, 36];

— применение антивирусного программного обеспечения и других средств защиты от киберугроз [4, 26].

3. Пожарная безопасность — меры по предотвращению возникновения пожаров и обеспечению безопасной эвакуации людей в случае их возникновения [10, 17]. Пожарная безопасность включает в себя:

— наличие и исправность средств пожаротушения, таких как огнетушители, пожарные гидранты и системы автоматического пожаротушения [17, 33];

— разработку и размещение планов эвакуации, обеспечивающих быстрый и организованный выход людей из здания в случае пожара [10, 33];

— проведение регулярных тренировок по эвакуации, позволяющих отработать действия в условиях чрезвычайной ситуации [41, 67].

4. Экологическая безопасность — обеспечение соответствия состояния окружающей среды требованиям, необходимым для безопасного пребывания людей на территории организации [41, 55]. Экологическая безопасность охватывает:

— контроль за качеством воздуха, воды и уровнем шума на территории образовательной организации [41, 67];

— меры по снижению негативного воздействия на окружающую среду, такие как утилизация отходов и использование экологически чистых материалов [41, 67].

5. Санитарно-эпидемиологическая безопасность — соблюдение требований санитарно-эпидемиологических норм и правил для обеспечения

здоровья участников образовательного процесса [41, 55]. Санитарно-эпидемиологическая безопасность включает в себя:

— регулярную дезинфекцию помещений, особенно в местах массового скопления людей [41];

— контроль за состоянием здоровья сотрудников и учащихся, включая проведение медицинских осмотров и профилактических мероприятий [41];

— соблюдение гигиенических норм, таких как поддержание чистоты и порядка в помещениях [41, 55].

6. Психологическая безопасность — создание комфортной и безопасной психологической атмосферы в образовательной организации [41, 67]. Психологическая безопасность способствует:

— предупреждению конфликтов и снижению уровня стресса среди участников образовательного процесса [41, 67];

— обеспечению психологического благополучия всех участников, что положительно сказывается на их общем состоянии и эффективности обучения [41, 67].

7. Транспортная безопасность — обеспечение безопасности при организации перевозок учащихся, особенно при использовании школьного транспорта [41, 53]. Транспортная безопасность включает в себя:

— проверку технического состояния транспортных средств перед каждым рейсом [41];

— контроль квалификации водителей, осуществляющих перевозку детей [41];

— соблюдение правил перевозки детей, обеспечивающих их безопасность во время движения [41, 53].

Обеспечение безопасности в образовательных организациях требует комплексного подхода, учитывающего все аспекты и виды безопасности, что позволяет создать безопасную и комфортную среду для всех участников образовательного процесса, способствующую эффективному обучению и

развитию, при этом специфика образовательных учреждений, такая как наличие большого количества несовершеннолетних, ограниченный доступ к определённым видам деятельности и необходимость соблюдения нормативных требований, накладывает особые условия на организацию безопасности.

1.2 Комплексные сети систем безопасности: понятие, структура и функции

Комплексные сети систем безопасности представляют собой интегрированные структуры, объединяющие различные подсистемы для обеспечения защиты объектов от потенциальных угроз [69]. Они включают в себя несколько ключевых компонентов, каждый из которых выполняет определённые функции.

Основными компонентами комплексных сетей систем безопасности являются:

— Средства идентификации и аутентификации — используются для подтверждения личности пользователей и предоставления им доступа к системе. К ним относятся пароли, биометрические данные, смарт-карты и токены [4, 29].

— Системы контроля доступа — обеспечивают управление доступом к ресурсам и зонам на основе политик безопасности, включая временные ограничения и уровни привилегий [38, 51].

— Системы обнаружения и предотвращения вторжений (IDS/IPS) — анализируют сетевой трафик в реальном времени, выявляя аномалии и признаки атак [26, 28].

— Антивирусные и антималварные системы — предназначены для обнаружения, блокировки и удаления вредоносного ПО (вирусы, трояны, шпионские программы и др.) [4, 26].

— Системы резервного копирования и восстановления данных — обеспечивают целостность информации и возможность восстановления после сбоев, утечек или атак [28, 36].

— Системы мониторинга и аудита безопасности — регистрируют события в логах, позволяя отслеживать действия пользователей и выявлять нарушения [28, 47].

— Межсетевые экраны (файерволы) — фильтруют сетевой трафик по заданным правилам, блокируя несанкционированный доступ [4, 26].

— Системы управления инцидентами и событиями безопасности (SIEM) — собирают и коррелируют данные из различных источников, обеспечивая централизованный анализ и оперативное реагирование [28, 36].

— Системы защиты от DDoS-атак — обнаруживают и смягчают распределённые атаки, направленные на отказ в обслуживании [26, 65].

Функции КССБ:

— Мониторинг состояния объектов в реальном времени с фиксацией всех событий: движение, открытие дверей, попытки несанкционированного доступа [10, 69].

— Автоматическая идентификация инцидентов (вторжения, пожары, утечки данных) с использованием правил корреляции событий и алгоритмов машинного обучения [28, 47].

— Анализ рисков и прогнозирование угроз на основе исторических данных и текущих трендов [1, 51].

— Централизованное управление всеми подсистемами безопасности с единой консоли [10, 35].

— Документирование и архивация событий для последующего расследования инцидентов [47, 69].

— Обеспечение кибербезопасности ИТ-инфраструктуры (защита от вирусов, DDoS-атак, несанкционированного доступа) [26, 44].

— Координация действий служб безопасности (охрана, IT-отдел, администрация) при ЧС [41, 67].

— Интеграция с внешними системами, такими как «Безопасный город», службы экстренного реагирования [10, 35].

В контексте образовательных учреждений КССБ должна учитывать специфику объекта:

— защита персональных данных обучающихся и сотрудников — в соответствии с требованиями ФЗ-152 [43, 60];

— контроль доступа в учебные корпуса и лаборатории — с учётом графика занятий и возрастных ограничений [38, 41];

— мониторинг безопасности лабораторного оборудования и IT-инфраструктуры — особенно в технических и IT-специальностях [36, 41];

— обеспечение антитеррористической защищённости кампуса — включая видеонаблюдение, контроль доступа и тревожные кнопки [17, 69];

— защита от киберугроз — фишинг, вредоносное ПО, атаки на LMS и электронные дневники [26, 67].

КССБ представляет собой интегрированную систему, объединяющую технические, программные и организационные средства для защиты объектов от различных угроз. Ключевой особенностью КССБ является единая платформа управления, позволяющая централизованно мониторить и реагировать на инциденты. Особая значимость КССБ подчёркивается при применении в образовательных организациях, где система должна обеспечивать не только физическую безопасность, но и защиту персональных данных, IT-инфраструктуры, антитеррористическую защищённость.

1.3 Инциденты в работе комплексных сетей систем безопасности: понятие и классификация

В контексте безопасности под инцидентом понимается любое незапланированное или нежелательное событие, способное нарушить целостность, доступность или конфиденциальность защищаемых информационных и материальных активов организации [6, 21]. Такое определение соответствует общепринятому подходу в области информационной безопасности и поддерживается нормативными документами и научными работами [47, 52].

В контексте образовательной организации такие инциденты могут затрагивать:

— ИТ инфраструктуру (серверы, рабочие станции, сетевое оборудование) [28, 36];

— системы контроля и управления доступом (СКУД) [38, 51];

— системы видеонаблюдения и охранной сигнализации [10, 69];

— каналы передачи данных и межсетевые взаимодействия [4, 26].

Инциденты могут иметь различный характер и источники, включая несанкционированный доступ, сбои в работе системы, утечки данных, атаки на программное обеспечение и другие угрозы [26, 44]. Эффективное управление безопасностью требует не только их выявления, но и систематизации — для этого применяется классификация инцидентов, позволяющая определить наиболее подходящие методы реагирования и профилактики [47, 69].

Основные критерии классификации инцидентов:

1) по источнику возникновения:

— внутренние инциденты возникают из-за ошибок персонала, сбоев в программном или аппаратном обеспечении, а также вследствие намеренных действий сотрудников с вредоносными целями (инсайдерские угрозы) [1, 41];

— внешние инциденты связаны с действиями злоумышленников — хакеров, ботнетов, киберпреступных групп — направленными на

несанкционированный доступ, выведывание данных или нарушение работы систем [26, 67];

2) по степени воздействия:

— низкоуровневые инциденты — например, ложное срабатывание сигнализации или временный сбой в работе одного рабочего места — имеют незначительное влияние и устраняются оперативно [47, 69];

— среднеуровневые инциденты — такие как атака фишинга на группу сотрудников или частичный сбой СКУД — требуют вмешательства специалистов и анализа логов [28, 41];

— высокоуровневые инциденты — включают масштабные утечки персональных данных, DDoS-атаки на образовательные платформы или физическое проникновение на территорию — представляют серьёзную угрозу и требуют включения плана реагирования на инциденты (ИРП) [47, 60, 67];

3) по времени обнаружения:

— незамеченные инциденты («тихие» атаки) остаются необнаруженными в течение длительного времени, что позволяет злоумышленникам устанавливать бэкдоры, собирать данные и маскировать свою активность [28, 67];

— своевременно обнаруженные инциденты выявляются с помощью SIEM-систем, IDS/IPS и других средств мониторинга, что позволяет минимизировать ущерб [28, 36];

— опоздавшие инциденты обнаруживаются уже после нанесения ущерба (например, после публикации утекших данных в даркнете), что требует проведения расследования и восстановительных мероприятий [47, 69];

4) по области возникновения:

— инциденты физической безопасности включают попытки несанкционированного проникновения, повреждение камер видеонаблюдения, отключение охранной сигнализации [10, 17, 69];

— инциденты информационной безопасности — утечки данных, вредоносное ПО, атаки на LMS, нарушение работы баз данных — требуют вмешательства ИТ-службы и применения технических мер защиты [26, 43, 60].

Понимание и систематическая классификация инцидентов в работе комплексных сетей систем безопасности (КССБ) позволяют:

— разработать эффективные стратегии предотвращения и реагирования на угрозы;

— оптимизировать распределение ресурсов служб безопасности;

— минимизировать время реакции и объём ущерба;

— обеспечить соответствие требованиям нормативных актов (ФЗ-152, ФЗ-187, РД ФСТЭК) [47, 53, 60].

Классификация служит основой для построения процедур выявления, анализа и устранения инцидентов, а также для обучения персонала и проведения учений по кибербезопасности [41, 67].

Выводы по первой главе

В первой главе исследованы теоретические основы обеспечения безопасности в образовательных организациях.

Установлено, что безопасность образовательной организации — это комплексное состояние защищённости участников образовательного процесса (жизнь, здоровье, психологическое благополучие), материальных и информационных активов, инфраструктуры и непрерывности учебного процесса.

Систематизированы основные виды безопасности: физическая, информационная, пожарная, экологическая, санитарно-эпидемиологическая, психологическая, транспортная. Их взаимосвязь требует комплексного подхода к проектированию защитных мер.

Определено, что комплексные сети систем безопасности — это интегрированная среда, объединяющая технические, программные и организационные компоненты для защиты от угроз. Ключевые характеристики:

— структура: аппаратный, программный и организационный уровни;

— функции: мониторинг в реальном времени, идентификация инцидентов, централизованное управление, документирование событий, координация служб;

— специфика для образовательных организаций: защита персональных данных, антитеррористическая защищённость, контроль доступа, киберзащита IT-инфраструктуры.

Комплексные сети систем безопасности обеспечивает синергетический эффект за счёт интеграции подсистем (видеонаблюдение, СКУД, SIEM, IDS/IPS и др.).

Инцидент в комплексных сетях систем безопасности трактуется как незапланированное событие, нарушающее целостность, доступность или конфиденциальность активов. Предложена классификация по критериям:

— источник: внутренний / внешний;

— степень воздействия: низкий / средний / высокий уровень ущерба;

— время обнаружения: своевременное / опоздавшее / незамеченное;

— область возникновения: физическая / информационная безопасность.

Такая типология служит основой для формализации индикаторов угроз, ранжирования рисков и разработки алгоритмов реагирования.

Теоретический анализ подтвердил, что эффективное обеспечение безопасности в образовательной организации требует:

— учёта всех видов безопасности в их взаимосвязи;

— внедрения комплексных сетей систем безопасности как инструмента комплексной защиты;

— систематизации инцидентов для проектирования методик их выявления и устранения.

Полученные результаты составляют теоретическую базу для последующих этапов исследования — разработки методического обеспечения выявления инцидентов с учётом специфики образовательных организаций.

ГЛАВА 2. МЕТОДЫ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ В РАБОТЕ КОМПЛЕКСНЫХ СЕТЕЙ СИСТЕМ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ КОЛЛЕДЖ»

2.1 Общие сведения об ГБПОУ «Южно-Уральский государственный колледж»

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа.

Главной целью и направлением деятельности образовательной организации является повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на системе электронного обучения E-Learning, электронных учебно-методических комплексах, а также компетентностном подходе. Данные технологии и формы обучения позволили повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда. На протяжении многих лет «Южно-Уральский государственный колледж» занимается разработкой и внедрением в учебном процессе интенсивных информационных образовательных технологий, основанных на широком использовании компьютерной и коммуникационной техники, электронных обучающих программ, проектной культуры. Это позволяет активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России.

Педагоги колледжа имеют опыт практической работы и глубокую теоретическую подготовку, необходимую для успешной реализации профессиональных образовательных программ. Среди них — кандидаты

наук, заслуженные работники образования Российской Федерации, преподаватели высшей категории.

Для эффективного взаимодействия с учетом большого контингента обучающихся и месторасположением учебных зданий после реорганизации были присоединены два колледжа ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики» и ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики», которые в дальнейшем определили три образовательных комплекса:

— Информационных технологий и экономики (ул. Курчатова, д.7).

— Промышленной автоматики (ул. Доватора, д.38).

— Промышленного дизайна и торговли (ул. Блюхера, ул.1А).

В образовательной организации обоснованно распределены функции структурных подразделений учреждения, а также должностные обязанности его работников на основе сочетания принципов единоначалия и коллегиальности.

ГБПОУ «ЮУГК» возглавляет директор, обеспечивающий системную работу организации, определяющий стратегию, цели, задачи и программу его развития, обеспечивающий соблюдение законности в деятельности колледжа, а также осуществляющий иные функции и полномочия, соответствующие уставным целям.

По основным направлениям деятельности управление осуществляется заместителями директора, координирующими работу структурных подразделений ГБПОУ «ЮУГК».

В колледже действуют предметно-цикловые комиссии, деятельность, осуществляющих образовательную деятельность по родственным учебным дисциплинам/модулям, в том числе по совместительству. ГБПОУ «ЮУГК» уделяет большое внимание компьютеризации образовательного процесса.

В колледже оборудованы специализированные лаборатории и студии, для всех направлений обучения.

Для оптимизации учебной деятельности организация владеет всеми необходимыми современными программными пакетами: Microsoft Visio, Cisco Packet Tracer, Microsoft Visual Studio, Dev C++, SASM, Microsoft SQL Server 2017, SQL Management Studio, Android Studio, CorelDraw X4, Atom, Notepad++, Corel Photo Paint, Blender, Unity, Adobe Flash Professional CS6, Open Server, Oracle Virtual Box, IntelliJ IDEA, JDK, Free Pascal, Inkscape, GIMP, 1С Предприятие.

Используются 33 электронных курса по учебным дисциплинам, междисциплинарным курсам и профессиональным модулям.

При подготовке специалистов по всем реализуемым основным образовательным программам используются электронные системы обучения (электронные учебники, электронные таблицы, презентации отдельных тем и предметов, лабораторные и практические работы, обучающие программы на дисках, тестовый контроль).

Система управления ГБПОУ «ЮУГК», обеспечивающая реализацию образовательных программ, являющихся основной целью деятельности учреждения, отвечает требованиям действующего законодательства Российской Федерации и Челябинской области. Организационная структура управления ГБПОУ «Южно-Уральский государственный колледж» (рисунок 5).

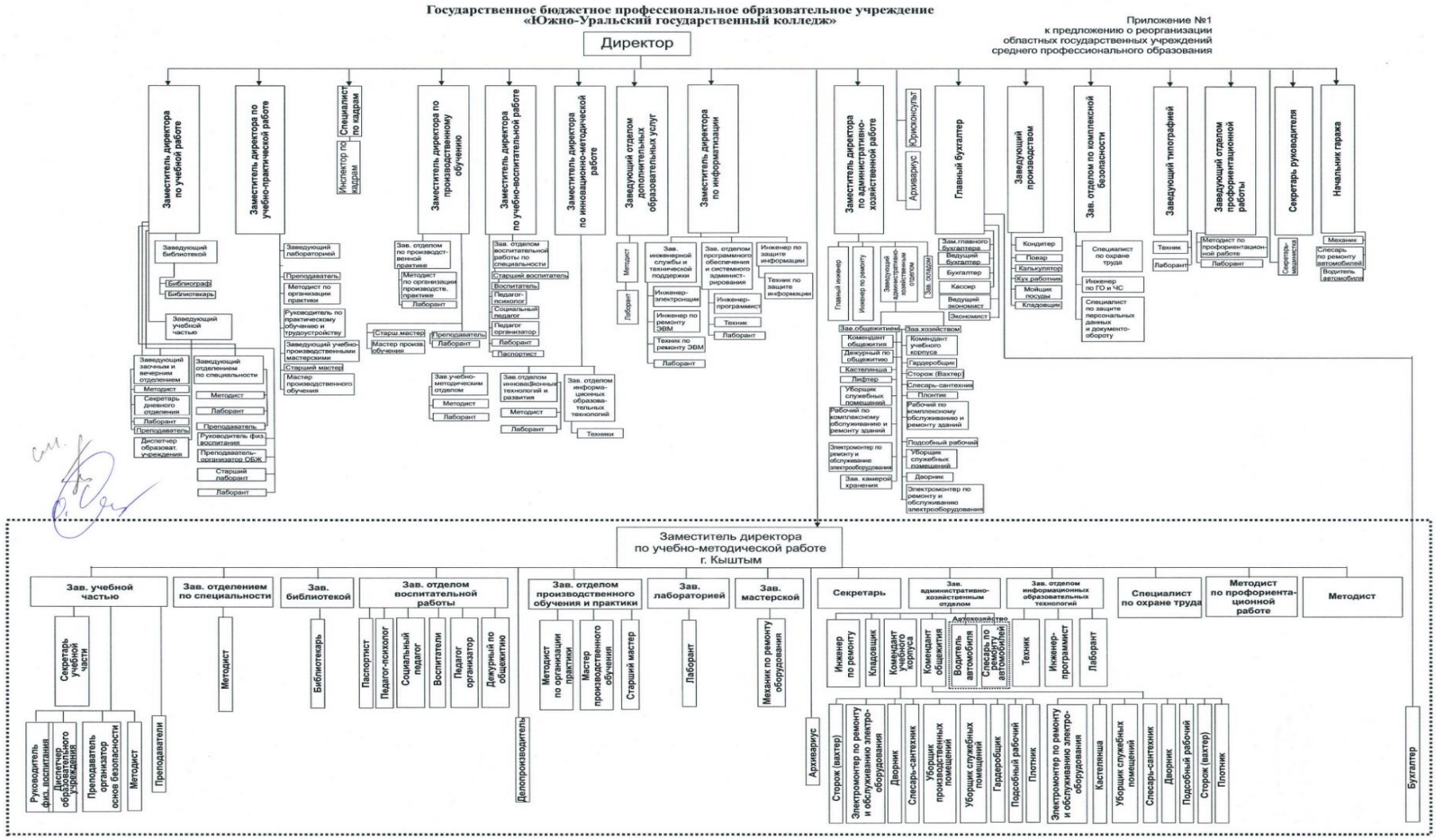

Рисунок 5 – Организационная структура управления ГБПОУ «Южно-Уральский государственный колледж»

2.2 Анализ существующих методов выявления инцидентов в ГБПОУ «ЮУГК»

В рамках исследования проведён анализ применяемых в ГБПОУ «ЮУГК» методов выявления инцидентов, затрагивающих комплексную сеть систем безопасности (КССБ). Цель анализа — оценить их эффективность, выявить пробелы и определить направления совершенствования методического обеспечения.

На момент исследования в ГБПОУ «ЮУГК» используются следующие методы:

1) ручной мониторинг журналов событий:

— операторы службы безопасности ежедневно просматривают логи СКУД, видеонаблюдения;

— фиксируются факты несанкционированного доступа, срабатывания сигнализации, сбои оборудования;

— ограничение: высокая трудоёмкость, риск пропуска аномалий из-за человеческого фактора [28, 47];

2) реактивное реагирование на обращения:

— инциденты выявляются по жалобам сотрудников, студентов или родителей (например, случаи вандализма, сбои в работе Wi-Fi);

— недостаток: запоздалое обнаружение, отсутствие превентивных мер [41, 67];

3) периодические проверки оборудования:

— еженедельный осмотр камер, датчиков, серверов, проверка актуальности антивирусных баз;

— слабое место: не позволяет выявлять скрытые инциденты (например, попытки подбора паролей) [28, 36];

4) автоматизированные оповещения от отдельных подсистем:

— срабатывание охранной сигнализации, уведомления о критических ошибках в ИТ-системах;

— проблема: отсутствие интеграции — оповещения поступают разрозненно, без корреляции между подсистемами [28, 36].

Анализ показал следующие системные недостатки:

— фрагментированность данных: информация из СКУД, ИТ-инфраструктуры и видеонаблюдения не консолидируется, что затрудняет реконструкцию событий и расследования инцидентов [28, 35];

— отсутствие проактивных механизмов: большинство инцидентов обнаруживается постфактум (например, утечки данных или внутренние злоупотребления) [43, 60];

— низкая скорость реагирования: ручное сопоставление данных увеличивает время локализации угрозы, что противоречит требованиям оперативности [47, 69];

— недостаточная детализация отчётов: журналы событий не содержат метаданных (IP-адреса, геолокация), необходимых для расследования [28, 47];

— ограниченная аналитика: отсутствуют инструменты для выявления паттернов, таких как повторяющиеся попытки доступа в нерабочее время, что может указывать на инсайдерские угрозы [1, 41].

Существующие методы в ГБПОУ «ЮУГК» ориентированы преимущественно на реактивное выявление инцидентов и не соответствуют современным требованиям к комплексной безопасности. Для перехода к проактивной модели необходимо:

— внедрить SIEM-систему для корреляции событий из всех подсистем КССБ (СКУД, ИТ, видеонаблюдение, антивирусы) [28, 36];

— разработать алгоритмы анализа аномалий (на основе машинного обучения или правил для выявления скрытых угроз) [1, 41];

— стандартизировать шаблоны отчётов с указанием критичности инцидента (низкая, средняя, высокая), источника, времени и рекомендуемых действий [47, 69];

— организовать регулярное обучение персонала методам работы с интегрированными системами [41, 67].

Таким образом, текущая практика требует модернизации методического обеспечения — от разрозненных процедур к единой системе выявления и реагирования на инциденты, учитывающей специфику образовательной среды и нормативные требования (ФЗ № 152, ФЗ № 35).

2.3 Алгоритм выявления инцидентов

В условиях цифровизации образования и роста числа киберугроз критически важно внедрять формализованные алгоритмы выявления инцидентов информационной безопасности [26, 41]. Такие алгоритмы должны обеспечивать своевременное, достоверное и полное обнаружение угроз при минимизации ложных срабатываний и человеческого фактора, а также учитывать специфику инфраструктуры и процессов образовательных организаций [47, 69].

1. Концептуальные основы алгоритма

Алгоритм базируется на следующих принципах:

— комплексность — охват всех типов угроз (утечки данных, кибератаки, сбои, несанкционированный доступ, фишинг) [1, 28];

— интеграция данных — объединение информации из разнородных источников (SIEM, IDS/IPS, DLP, СКУД, LMS, облачные сервисы, почтовые серверы) [28, 36];

— многоуровневость анализа — сочетание логического анализа, статистических методов и машинного обучения [41, 60];

— адаптивность — настройка под специфику организации (график занятий, контингент, ИТ-ландшафт) [47, 69];

— прозрачность и прослеживаемость — фиксация всех этапов для аудита и расследований [28, 47];

— соответствие нормативной базе — соблюдение требований ФЗ № 152, ФЗ № 187, ГОСТ Р ИСО/МЭК 27001 и др. [43, 53, 60];

— экономическая целесообразность — баланс между функциональностью и стоимостью для бюджетных организаций [26, 41].

2. Пошаговый алгоритм выявления инцидентов

Шаг 1. Сбор данных:

— автоматический сбор логов (периодичность — каждые 5 мин; форматы — JSON, CSV, Syslog);

— ручной ввод информации (обращения пользователей, результаты аудитов) — в течение 1 часа после события;

— источники: сетевые устройства, серверы, рабочие станции, LMS, СКУД, облачные сервисы [28, 36].

Шаг 2. Нормализация и фильтрация:

— унификация временных меток, идентификаторов объектов, кодов событий;

— исключение неинформативных записей (штатные операции);

— агрегация повторяющихся событий [28, 36].

Шаг 3. Первичная классификация:

— определение типа инцидента (утечка, атака, сбой, несанкционированный доступ и т. д.);

— присвоение предварительной степени критичности (низкая/средняя/высокая) на основе: задействованных активов (персональные данные, критичные серверы); потенциального ущерба (финансового, репутационного, правового) [47, 69].

Шаг 4. Анализ и корреляция

Применяются три взаимодополняющих метода:

— логический анализ — сопоставление с известными сигнатурами угроз (например, шаблоны фишинговых писем, IP-адреса ботнетов) [1, 28];

— статистические методы — выявление аномалий в больших объёмах данных (например, отклонение сетевого трафика от нормы, массовая выгрузка файлов) [41, 60];

— машинное обучение — адаптация к новым типам угроз и выявление сложных закономерностей (например, нетипичное поведение учётной записи) [41, 67].

Дополнительно используется User Behavior Analytics (UBA) для анализа активности пользователей (студенты, преподаватели, персонал) и выявления отклонений от «нормального» поведения [1, 67].

Шаг 5. Приоритизация

На основе матрицы рисков (ущерб × вероятность) инцидент получает итоговую степень критичности:

— высокая — немедленное реагирование (например, подтверждённая утечка персональных данных);

— средняя — обработка в течение 2 часов;

— низкая — плановый разбор (например, единичная ошибка аутентификации) [47, 69].

Шаг 6. Эскалация и уведомление:

— автоматическое оповещение ответственных (администратор ИБ, служба безопасности);

— передача в внешние системы (например, ГосСОПКА при подтверждении кибератаки);

— уведомление Роскомнадзора при утечках персональных данных (в соответствии с ФЗ № 152) [43, 60].

Шаг 7. Фиксация и документирование

Заполнение шаблона отчёта с полями: тип инцидента; степень критичности; задействованные подсистемы и активы; время обнаружения и фиксации; рекомендуемые меры реагирования; статус (в работе/устранён/эскалирован) [28, 47].

Архивирование логов и метаданных для последующего анализа.

Шаг 8. Реагирование и устранение:

— изоляция затронутых активов (например, блокировка учётной записи, отключение порта);

— нейтрализация угрозы (удаление вредоносного ПО, восстановление данных из резервной копии);

— устранение причин (установка патчей, корректировка прав доступа) [47, 69].

Шаг 9. Пост-инцидентный анализ:

— разбор причин возникновения инцидента;

— оценка эффективности реагирования;

— корректировка правил корреляции и сигнатур угроз;

— обновление чек-листов и регламентов;

— планирование мероприятий по недопущению аналогичных инцидентов [47, 69].

Шаг 10. Мониторинг и адаптация:

— регулярный пересмотр алгоритма (каждые 3 месяца);

— обучение моделей машинного обучения на новых данных;

— проведение учений (имитация атак) 1 раз в полугодие [41, 67].

3. Обзор аналогов алгоритмов и систем

Для реализации алгоритма применяются следующие классы решений:

1. Системы обнаружения и предотвращения вторжений (IDS/IPS):

— PT NAD (Positive Technologies) — глубокая инспекция трафика (DPI), интеграция с MaxPatrol SIEM, автоматическое выявление аномалий, поддержка протоколов IIoT, SCADA, сертификация ФСТЭК [28];

— «Рубикон» (НПО «Эшелон») — сочетание сигнатурного анализа, поведенческих моделей и ML-алгоритмов; обогащение событий контекстом, формирование цепочек атак [41];

— «Аргус» («Центр Специальной Системотехники») — анализ приложений и протоколов на уровне полезной нагрузки, ориентирован на сегменты с плотным трафиком [36];

— ViPNet IDS NS (ИнфоТеКС) — обнаружение атак на основе сигнатур и эвристики, глубокий анализ трафика (DPI), интеграция с ViPNet Coordinator [47].

2. SIEM-системы:

— MaxPatrol SIEM — централизованное управление безопасностью ИТ-инфраструктуры, динамическая группировка активов, интеграция с другими продуктами Positive Technologies [28];

— KUMA («Лаборатория Касперского») — защита от сложных целевых атак, интеграция с Kaspersky Anti Targeted Attack Platform и Kaspersky EDR [41];

— RuSIEM — высокая производительность (до 90 000 событий/сек на одном узле), сохранение сырых событий для форензики, масштабируемость [41];

— Security Capsule SIEM — легковесное решение с быстрым созданием правил корреляции; внедрено в ряде образовательных учреждений для аудита логов учебных платформ [69].

3. Решения с элементами машинного обучения и UBA:

— ViPNet TIAS (ИнфоТеКС) — корреляция событий из разных источников (IDS, SIEM, endpoint), автоматическое построение цепочек атак с анализом по модели MITRE ATT&CK [47];

— UBA-модули в составе SIEM/DLP — анализ поведения пользователей для выявления подозрительной активности (например, вход в систему в нерабочее время, массовая выгрузка данных) [1, 67].

Для образовательных организаций СПО с ограниченными ИТ-бюджетами критически важно внедрять экономически целесообразные алгоритмы выявления инцидентов, обеспечивающие базовый уровень защиты при минимальных затратах. Ниже представлен поэтапный алгоритм, адаптированный под специфику образовательных организаций СПО: ограниченные кадровые ресурсы, разнородную пользовательскую

базу (студенты, преподаватели, администрация) и ценность персональных данных.

Алгоритм строится на следующих принципах:

— минимальные начальные затраты — использование open-source-решений и встроенных средств ОС;

— простота эксплуатации — минимизация требований к квалификации персонала;

— поэтапное внедрение — масштабирование по мере роста зрелости ИБ-процессов;

— соответствие нормативным требованиям — выполнение обязательств по ФЗ № 152 «О персональных данных»;

— фокус на приоритетные угрозы — утечки данных, фишинг, несанкционированный доступ, сбои инфраструктуры [26, 41].

Пошаговый алгоритм

Шаг 1. Инвентаризация активов и рисков

— составить реестр ИТ-активов (серверы, рабочие станции, LMS, СКУД, сетевые устройства);

— определить критичные данные (персональные данные студентов/сотрудников, академические записи);

— выделить типовые угрозы (например, несанкционированная выгрузка данных через USB, фишинговые атаки на почту) [47, 69].

Шаг 2. Внедрение базовых технических мер:

— активировать встроенные средства аудита ОС (Windows Event Log, Syslog в Linux) для фиксации входов, изменений прав доступа, запуска ПО;

— настроить брандмауэр на серверах и рабочих станциях (блокировка подозрительных соединений, запрет нештатных портов);

— развернуть антивирусное ПО с централизованным управлением (например, Kaspersky Endpoint Security в базовой конфигурации) [4, 26].

Шаг 3. Сбор и первичная обработка данных:

— организовать автоматический сбор логов с ключевых узлов (сервер каталога, почтовый сервер, LMS) через Syslog-агент (например, NXLog Community Edition);

— настроить фильтрацию неинформативных записей (штатные операции, ошибки низкого уровня);

— агрегировать события в централизованном хранилище (например, на выделенном файловом сервере с ограниченным доступом) [28, 36].

Шаг 4. Анализ аномалий и выявление инцидентов:

— использовать простые правила корреляции (например, множественные неудачные попытки входа → подозрение на подбор пароля);

— внедрить статистический мониторинг сетевого трафика (например, через ntopng — бесплатный анализатор с веб-интерфейсом);

— применять контент-анализ почтовых сообщений на ключевые слова («пароль», «перевести деньги» и т. п.) через скрипты на Python/PowerShell [41, 67].

Шаг 5. Приоритизация и эскалация:

1) классифицировать инциденты по трём уровням:

— высокий (подтверждённая утечка, компрометация учётной записи) → немедленное оповещение администратора;

— средний (подозрительная активность, аномальный трафик) → разбор в течение 4 часов;

— низкий (единичная ошибка аутентификации) → плановый анализ раз в неделю;

2) настроить автоматические уведомления через Telegram-бота или e-mail (например, с помощью скриптов на Python с библиотекой smtplib) [47, 69].

Шаг 6. Реагирование и документирование:

— изолировать затронутые активы (отключить порт коммутатора, заблокировать учётную запись);

— зафиксировать инцидент в журнале учёта (Excel/Google Sheets) с полями: дата/время обнаружения; тип инцидента; хронология событий; задействованные активы; принятые меры; статус (в работе/устранён/эскалирован); запланировать мероприятия по устранению и недопущению аналогичных инцидентов;

— восстановить работоспособность из резервных копий (резервное копирование критичных данных — ежедневно, хранение — на отдельном носителе) [43, 60].

Шаг 7. Пост-инцидентный анализ:

— провести разбор причин (опрос пользователей, анализ логов);

— обновить правила мониторинга (например, добавить новый шаблон подозрительной активности);

— провести мини-обучение персонала (1 раз в квартал):

— правила создания паролей;

— признаки фишинговых писем;

— порядок действий при подозрении на инцидент[41, 67].

Рекомендуемые инструменты (бюджетные/бесплатные)

1) Сбор и анализ логов:

— NXLog Community Edition (Syslog-агент);

— Graylog Open Source (централизованный сбор, простой поиск);

— PowerShell/Python-скрипты для парсинга логов [28, 36].

2) Сетевой мониторинг:

— ntopng (анализ трафика, выявление аномалий);

— Wireshark (ручной анализ подозрительных сессий) [41, 67].

3) Антивирусная защита:

— Kaspersky Endpoint Security (базовый тариф);

— Dr. Web Desktop Security Suite (специальные цены для образовательных учреждений) [4, 26].

4) Резервное копирование:

— Veeam Agent for Windows/Linux Free;

— встроенные средства ОС (Windows Backup, rsync в Linux) [43, 60].

Организационная поддержка:

— назначить ответственного за ИБ (администратор сети/преподаватель ИТ-дисциплин);

— разработать регламент реагирования (краткие инструкции для персонала: «Что делать при подозрении на утечку/вирус»);

— проводить ежеквартальные проверки (аудит прав доступа, обновление ПО, тестирование резервных копий) [41, 67].

Ключевые метрики для контроля:

— время обнаружения инцидента (TTD) — цель: ≤2 часа для угроз высокого уровня [47, 69];

— время реагирования (TTR) — цель: ≤4 часа для изоляции угрозы [47, 69];

— доля предотвращённых инцидентов — расчёт на основе журнала учёта [67];

— соответствие нормативным требованиям — проверка через внутренние аудиты (1 раз в полугодие) [43, 60].

Предложенный алгоритм позволяет образовательным организациям СПО:

— обеспечить базовый уровень защиты от наиболее вероятных угроз;

— минимизировать затраты за счёт open-source-решений и встроенных средств ОС;

— постепенно наращивать функциональность (например, переход от Graylog к SIEM при увеличении бюджета);

— выполнять обязательства по ФЗ № 152 без значительных капитальных вложений.

Ключевой фактор успеха — регулярность (мониторинг, обучение, аудит) и простота процессов, исключающая зависимость от

узкоспециализированных кадров [41, 67]. Эффективность системы безопасности в образовательной организации напрямую зависит не от количества внедрённых технологий, а от стабильности и предсказуемости процессов, что особенно важно при ограниченных ИТ-ресурсах [26, 47].

Для образовательных организаций с ограниченными бюджетами ключевыми критериями выбора систем выявления инцидентов ИБ являются стоимость, простота внедрения и достаточность функционала для базовых задач [26, 41]. Рассмотрим несколько бюджетных аналогов, которые могут быть применимы в таких условиях, и сравним их в Таблице 1.

Аналоги алгоритмов выявления инцидентов для КССБ образовательных организаций

ViPNet IDS HS — система обнаружения вторжений, которая осуществляет мониторинг и обработку событий внутри хоста. Использует сигнатурный и эвристический методы анализа атак на основе правил и сигнатур, разработанных в России. Централизованное управление агентами, настройками и группами правил на хостах позволяет администраторам оперативно реагировать на события безопасности в сети. Система сертифицирована ФСТЭК России и интегрируется с ViPNet Coordinator, что делает её пригодной для организаций, требующих соответствия отечественным стандартам информационной безопасности [47, 69].

Security Capsule SIEM — российская SIEM-система, сертифицированная ФСТЭК России [69]. Обеспечивает централизованный автоматизированный мониторинг событий, анализ и выявление инцидентов ИБ в режиме реального времени. Поддерживает интеграцию с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) через модуль «ГосСОПКА». Рассчитана на компании любого масштаба. Security Capsule SIEM внедрена в ряд образовательных учреждений для аудита логов учебных платформ и контроля доступа к персональным данным студентов [69].

R-Vision UEBA — программный продукт для непрерывного мониторинга событий безопасности [67]. Анализирует данные из систем Log Management, SIEM и конечных устройств [67]. Аналитические инструменты позволяют своевременно выявить признаки атаки, приоритизировать угрозы и анализировать последовательность аномальных событий. Особенно эффективен для выявления инсайдерских угроз и долгосрочных атак (APT), где традиционные сигнатурные методы оказываются недостаточными [1, 67]. R-Vision UEBA использует технологии User and Entity Behavior Analytics (UEBA), что соответствует современным подходам к проактивной кибербезопасности [67].

InfoWatch Traffic Monitor — DLP-система, которая предотвращает утечки конфиденциальных данных [1]. Контролирует все каналы передачи информации: электронная почта, мессенджеры, облачные хранилища, USB-порты, печать. Позволяет гибко настраивать политики фильтрации контента на основе ключевых слов, регулярных выражений, шаблонов документов (например, паспортные данные, зачётки) [43]. InfoWatch Traffic Monitor активно используется в образовательных организациях для защиты персональных данных студентов и преподавателей, что напрямую соответствует требованиям ФЗ № 152-ФЗ [43, 60].

Таблица 1 – Сравнительная таблица аналогов алгоритмов выявления инцидентов для КССБ образовательных организаций

Критерий	ViPNet IDS HS	Security Capsule SIEM	R-Vision UEBA	InfoWatch Traffic Monitor
Основной метод обнаружения	Сигнатурный и эвристический анализ	Корреляция событий из разных источников	Поведенческая аналитика (UEBA)	Контроль каналов передачи данных (DLP) IS.Astral.ru +3
Стоимость	Относительно невысокая за счёт фокуса на хост-защите	Доступна для организаций разного масштаба, включая бюджетные	Зависит от конфигурации и интеграции с другими системами	Может быть дороже из-за функционала DLP, но есть варианты лицензирования
Сложность внедрения	Требует настройки правил и интеграции с инфраструктурой	Требует времени на настройку правил корреляции, но имеет готовые шаблоны	Требует сбора исторических данных для обучения моделей	Относительно простое внедрение при наличии чётких политик безопасности
Ключевые преимущества	Локализация угроз на хостах, централизованное управление	Соответствие регуляторным требованиям, интеграция с НКЦКИ	Выявление инсайдерских угроз и аномалий	Эффективная защита от утечек данных
Недостатки	Ограниченная видимость сетевых угроз	Высокая ресурсоёмкость при больших объёмах данных	Длительный период обучения моделей, сложность интерпретации результатов	Риск нарушения приватности пользователей, ложные срабатывания
Применимость в образовательных организациях	Для защиты рабочих станций и серверов с персональными данными	Для крупных вузов с необходимостью соответствия регуляторным требованиям	Для выявления аномалий в поведении пользователей и устройств	Для предотвращения утечек конфиденциальных данных (например, персональных данных студентов)

При выборе системы стоит учитывать специфику образовательной организации: размер инфраструктуры, уровень подготовки ИБ-специалистов, требования к соответствию регуляторам и бюджет. Для небольших учреждений с ограниченными ресурсами ViPNet IDS HS или Security Capsule SIEM могут стать оптимальным выбором благодаря балансу цены и функциональности. R-Vision UEBA и InfoWatch Traffic Monitor подойдут для организаций, где критически важно выявление аномалий или защита от утечек, но требуют более тщательной подготовки к внедрению.

Для образовательных организаций СПО оптимальным выбором является Security Capsule SIEM — она сочетает низкую стоимость, простоту внедрения, поддержку ГосСОПКА и соответствие российским стандартам [69].

Таким образом, разработанный алгоритм выявления инцидентов включает последовательность шагов, направленных на сбор, анализ, классификацию данных и реагирование на угрозы. Каждый шаг алгоритма обоснован и направлен на обеспечение эффективной защиты образовательных организаций от потенциальных угроз. В Приложении 1 приведена ситуация разбора инцидента по предложенному алгоритму.

Выводы по второй главе

ГБПОУ «ЮУГК» — многопрофильная образовательная организация с распределённой инфраструктурой (3 комплекса), интенсивной цифровизацией учебного процесса и значительным объёмом персональных данных. Это формирует повышенные требования к защите ИТ-инфраструктуры от кибератак, предотвращению утечек персональных данных студентов и сотрудников, обеспечению непрерывности образовательного процесса.

В ходе рассмотрения методов выявления инцидентов в работе комплексных сетей систем безопасности ГБПОУ «ЮУГК» выявлена существенная проблема: применяемые на текущий момент подходы носят преимущественно реактивный характер и не обеспечивают должного уровня проактивной защиты. Существующие практики — ручной мониторинг журналов, реагирование на обращения, периодические проверки и разрозненные автоматизированные оповещения — характеризуются значительными ограничениями: высокой трудоёмкостью, риском пропуска угроз из-за человеческого фактора, запоздалым обнаружением инцидентов и отсутствием интеграции между подсистемами. Это приводит к фрагментации данных, замедлению реагирования, недостаточной детализации отчётов и слабой аналитической базе.

В качестве решения предложен комплексный алгоритм, охватывающий полный цикл работы с инцидентами — от сбора данных до пост-инцидентного анализа. Алгоритм построен на принципах комплексности, интеграции данных, многоуровневого анализа, адаптивности и соответствия нормативным требованиям (ФЗ № 152, ФЗ № 187, ГОСТ Р ИСО/МЭК 27001). Он включает последовательные шаги: сбор и нормализация данных, первичная классификация, корреляционный анализ с применением логического, статистического и машинного методов, приоритизация угроз, эскалация, документирование, реагирование и

последующий разбор. Особое внимание уделено поведенческой аналитике (UBA) для выявления отклонений в активности пользователей и механизмам адаптации под специфику образовательной среды.

Для реализации алгоритма рассмотрены различные классы решений: IDS/IPS-системы (PT NAD, «Рубикон», ViPNet IDS NS), SIEM-платформы (MaxPatrol SIEM, KUMA, RuSIEM, Security Capsule SIEM) и инструменты с элементами машинного обучения (ViPNet TIAS, UBA-модули). При этом подчёркнута необходимость экономически целесообразного подхода для организаций с ограниченным бюджетом: предложены бюджетные аналоги (NXLog Community Edition, Graylog Open Source, ntopng, Kaspersky Endpoint Security, Veeam Agent Free), а также рекомендации по поэтапному внедрению — от базовых мер (инвентаризация активов, активация встроенных средств аудита, настройка брандмауэра) до постепенного масштабирования функционала.

Эффективность предложенного подхода можно оценить по ключевым метрикам: времени обнаружения (TTD ≤ 2 часа для угроз высокого уровня), времени реагирования (TTR ≤ 4 часа), доле предотвращённых инцидентов и соответствию нормативным требованиям. Важнейшими факторами успеха названы регулярность мониторинга, обучения персонала и проведения аудитов, а также простота процессов, снижающая зависимость от узкоспециализированных кадров. В целом, внедрение описанного алгоритма позволит ГБПОУ «ЮУГК» перейти к проактивной модели защиты, минимизировать риски утечек и кибератак, обеспечить соответствие законодательным требованиям и сохранить доверие участников образовательного процесса при разумных затратах.

ГЛАВА 3. ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРОЦЕССА ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ ГБПОУ «ЮУГК»

3.1 Разработка методического обеспечения процесса выявления инцидентов

Современные образовательные организации сталкиваются с ростом числа киберугроз: от фишинга и DDoS-атак до попыток хищения персональных данных обучающихся и сотрудников. В этих условиях критически важно разработать структурированное методическое обеспечение, учитывающее специфику деятельности и инфраструктуры образовательных учреждений. Как отмечается в исследованиях, такое обеспечение должно включать как предложение новых методов, так и усовершенствование существующих.

Цель разработки — создание унифицированной системы правил, процедур и инструментов, позволяющих: оперативно фиксировать признаки инцидентов; минимизировать влияние человеческого фактора; обеспечить преемственность действий ответственных лиц; сформировать доказательную базу для последующего анализа и предотвращения повторных угроз.

1. Цели и задачи разработки

Основная цель — формирование воспроизводимой методологии, обеспечивающей:

— оперативное обнаружение аномалий и угроз в КССБ;

— стандартизацию действий персонала при анализе событий;

— снижение влияния человеческого фактора на принятие решений;

— соответствие требованиям регуляторов (ФСТЭК, ФСБ, Минпросвещения, РКН) [43, 47, 60].

Задачи:

— систематизация типовых инцидентов и сценариев их проявления;

— разработка критериев идентификации угроз;

— формализация процедур мониторинга и анализа;

— создание шаблонов документации для фиксации и отчётности.

2. Нормативно-правовая основа.

Методическое обеспечение базируется на следующих нормативных документах:

— ФЗ № 152 «О персональных данных» (регулирует обработку и защиту персональных данных обучающихся и сотрудников) [43];

— ФЗ № 187 «О безопасности критической информационной инфраструктуры» (при наличии значимых объектов КИИ) [60];

— ФЗ № 149 «Об информации, информационных технологиях и о защите информации» [43];

— приказы и методические рекомендации ФСТЭК России (методы и средства защиты информации, аттестация объектов) [47, 69];

— требования Роскомнадзора по защите персональных данных [43, 60];

— внутренние регламенты организации (положение об ИБ, порядок обработки ПДн, должностные инструкции).

Эти документы задают обязательные требования к классификации инцидентов, срокам реагирования, формам отчётности, порядку взаимодействия с внешними структурами [47, 69].

3. Классификация инцидентов.

С учётом специфики образовательной среды выделяются следующие типовые категории инцидентов:

1) несанкционированный доступ к информационным ресурсам (взлом учётных записей, обход аутентификации) [1, 28];

2) утечка персональных данных обучающихся, сотрудников или иных субъектов ПДн [43];

3) заражение вредоносным ПО (вирусы, трояны, шифровальщики, ботнеты) [28, 67];

4) фишинговые атаки на персонал и учащихся (поддельные письма, сайты, SMS) [1, 41];

5) сбои в работе ИТ-инфраструктуры (аварийные, программные, аппаратные) [36, 47];

6) нарушение целостности данных (подмена, удаление, некорректное изменение) [47];

7) попытки обхода контент-фильтрации (доступ к запрещённым ресурсам) [26, 41];

8) некорректные действия пользователей (ошибки, халатность, нарушение регламентов) [47, 69].

Для каждой категории определяются критерии приоритета:

— высокий (угроза конфиденциальности/целостности, утечка ПДн, шифровальщики). Требует немедленного реагирования [43, 69];

— средний (сбои в работе сервисов, фишинг без последствий, единичные нарушения). Реагирование в течение 1–4 часов [47];

— низкий (ложные срабатывания, незначительные ошибки пользователей). Реагирование до 24 часов [69].

Такая классификация обеспечивает единообразие оценки и позволяет оптимизировать распределение ресурсов при реагировании.

4. Процедуры выявления.

Процесс выявления строится на комбинации источников данных и методов мониторинга:

Источники данных:

— журналы событий ОС, приложений, сетевого оборудования;

— отчёты систем защиты (антивирусы, DLP, SIEM, IDS/IPS);

— обращения пользователей (жалобы на сбои, подозрительную активность);

— результаты аудитов (прав доступа, конфигураций, уязвимостей);

— сканирования инфраструктуры (сетевые, веб-приложений, баз данных).

Методы мониторинга:

— реал-тайм — для критических систем (АСУ, базы ПДн);

— ежедневный — для журналов безопасности и оповещений SIEM;

— еженедельный — для аудита прав доступа и конфигураций;

— ежемесячный — для сканирования уязвимостей и тестирования на проникновение.

5. Алгоритм реагирования.

Пошаговый план действий при обнаружении инцидента:

1) Фиксация факта (дата, время, источник, симптомы, затронутые ресурсы).

2) Первичная оценка (масштаб, приоритет, предварительный тип инцидента).

3) Изоляция (отключение узла от сети, блокировка учётных записей, правил МЭ).

4) Уведомление (руководство, ИТ-отдел, служба безопасности, ГосСОПКА — при необходимости).

5) Сбор доказательств (копирование логов, скриншотов, дампов памяти).

6) Расследование (анализ причин, хронологии, ущерба).

7) Устранение (нейтрализация угрозы, восстановление систем).

8) Отчётность (оформление первичных и итоговых документов).

9) Профилактика (корректировка регламентов, обучение, обновление ПО).

Каждый этап сопровождается чек-листами для ответственных лиц, что снижает вероятность ошибок.

6. Документация и отчётность.

Обязательные формы отчётности:

— журнал регистрации инцидентов (номер, дата, описание, ответственные, статус);

— первичный отчёт (фиксация признаков, предпринятые меры, оценка ущерба);

— итоговый отчёт по расследованию (хронология, причины, рекомендации).

Критерии качества отчётов:

— полнота (все поля заполнены);

— точность (подтверждённые данные, без предположений);

— своевременность (в течение 24 ч после обнаружения);

— юридическая корректность (соответствие требованиям ФЗ и внутренних регламентов).

7. Обучение и тренировки.

Для повышения эффективности реагирования внедряются:

— ежегодные инструктажи для сотрудников и ИТ-персонала;

— имитационные учения по сценарию типовых инцидентов;

— памятки для учащихся о правилах безопасного поведения в сети;

— разбор кейсов прошлых инцидентов (анализ ошибок и успехов);

— тестирование знаний (опросы, симуляции фишинговых атак).

Формы обучения: очные семинары, онлайн-курсы, практические тренинги, вебинары с экспертами.

8. Критерии оценки эффективности.

Эффективность методического обеспечения оценивается по следующим показателям:

— среднее время обнаружения инцидента: ≤1 час [47, 69];

— доля ложных срабатываний: ≤5 % [41];

— полнота заполнения отчётов: 100 % [47];

— выполнение плана реагирования: ≥95 % [69];

— удовлетворённость участников процесса (по опросам): ≥80 % [67].

Дополнительно анализируется:

— динамика числа инцидентов по категориям;

— время восстановления после сбоев;

— количество предотвращённых угроз благодаря обучению [41, 67].

9. Интеграция с внешними системами.

Для усиления защиты предусматривается:

— подключение к ГосСОПКА (обмен информацией о кибератаках) [60, 69];

— взаимодействие с территориальными подразделениями МВД/ФСБ (при серьёзных угрозах) [47];

— обновление баз сигнатур угроз через официальные каналы поставщиков ПО [28, 47];

— участие в отраслевых рабочих группах по ИБ (обмен лучшими практиками) [41, 67].

10. Научно-методическая значимость.

Разработанное методическое обеспечение обладает следующими преимуществами:

— системность — объединяет технические, организационные и образовательные меры [47, 69];

— адаптивность — допускает корректировку под специфику организации [26, 41];

— проактивность — включает элементы превентивной защиты [67];

— документированность — обеспечивает юридическую прозрачность [47];

— масштабируемость — может применяться в организациях разного уровня [26, 41].

Ключевой принцип — баланс между автоматизацией и человеческим контролем. Технические средства (SIEM, антивирусы) выполняют

первичную фильтрацию данных, а ответственные лица принимают решения на основе чётких критериев и алгоритмов [47, 69].

Таким образом, методическое обеспечение процесса выявления инцидентов для КССБ образовательных организаций выступает как комплексный инструмент управления рисками, сочетающий:

— нормативно-правовую основу;

— типовые процедуры и алгоритмы;

— стандартизированные формы отчётности;

— механизмы обучения и контроля.

Его внедрение позволяет не только оперативно реагировать на текущие угрозы, но и накапливать базу знаний для совершенствования системы информационной безопасности в долгосрочной перспективе. Разработанное решение соответствует современным требованиям ИБ и может служить основой для тиражирования в других образовательных организациях.

3.2. Методические и технические решения по автоматизации выявления инцидентов

Для повышения точности и оперативности выявления инцидентов в комплексных сетях систем безопасности (КССБ) образовательной организации предложены три ключевых алгоритма автоматизации:

— корреляция событий — сопоставление данных из разных источников (например, попытка входа с неизвестного IP + срабатывание IDS → потенциальная атака) [47, 69];

— анализ аномалий — выявление отклонений от «нормального» поведения (например, массовая выгрузка данных в нерабочее время, множественные неудачные попытки входа) [67];

— прогнозирование угроз — на основе исторических данных и индикаторов компрометации (IoC) (например, рост числа фишинговых писем → повышение уровня защиты почтового шлюза) [41, 67].

Такие подходы позволяют перейти от реактивного к проактивному управлению инцидентами, что особенно важно в условиях ограниченных ИТ-ресурсов и высокой цифровой нагрузки в образовательной среде [26, 47].

Техническая реализация алгоритмов предполагает использование следующих компонентов:

— SIEM-системы (MaxPatrol SIEM, Kaspersky Unified Monitoring) — для централизованного сбора, корреляции и анализа событий [69];

— IDS/IPS (Suricata, Snort) — для мониторинга сетевого трафика и блокировки атак [47];

— DLP-решения (InfoWatch, Solar Dozor) — для предотвращения утечек данных [43, 60];

— сканеры уязвимостей (Nessus, OpenVAS, XSpider) — для регулярного аудита инфраструктуры [41, 60].

Такой подход обеспечивает комплексный охват как технических, так и организационных аспектов информационной безопасности, формируя основу для построения единой системы управления инцидентами.

Внедрение предложенного методического обеспечения осуществляется в четыре этапа:

Подготовка (1–2 недели): аудит ИТ-инфраструктуры, обучение персонала, настройка интеграционных шлюзов.

Пилотное тестирование (1 месяц): апробация на ограниченном сегменте (например, серверной инфраструктуре), сбор обратной связи, корректировка правил корреляции.

Масштабирование (2–4 недели): развёртывание на всей территории организации, интеграция с внешними системами (СКУД, LMS, почтовыми серверами).

Мониторинг и адаптация (постоянно): пересмотр правил каждые 3 месяца, обновление отчётов, проведение учений (имитация атак) раз в полгода.

Ожидаемые результаты и практическая значимость:

— сокращение времени обнаружения инцидентов ИБ на 40,0–60,0 % за счёт автоматизации [47, 69];

— снижение ошибок из-за человеческого фактора на 50,0–70,0 % [41, 67];

— единый формат учёта и расследования (прозрачность решений) [47];

— минимизацию ущерба от угроз (финансового, репутационного, правового) [43, 60];

— соответствие нормативным требованиям (ФЗ № 152, ФЗ № 187 и нормативам ФСТЭК) [43, 60, 69].

Кроме того, система создаёт основу для единой системы управления инцидентами ИБ в образовательной организации и может быть адаптирована для других учреждений с учётом их ИТ-ландшафта [26, 41, 69].

Для оценки эффективности предложены ключевые показатели эффективности (KPI):

— среднее время обнаружения инцидента (целевой показатель: ≤ 10 мин для высокой критичности);

— доля выявленных угроз от общего числа (целевой показатель: ≥ 95,0%);

— количество ложных срабатываний (оптимально: ≤ 5,0 % от всех оповещений)

— время устранения инцидента (целевой показатель: ≤ 2 часа для высокой критичности);

— удовлетворённость персонала (опросы каждые 6 месяцев).

Разработанное методическое обеспечение представляет собой целостную систему, сочетающую:

— технические возможности КССБ (SIEM, IDS, DLP и др.);

— стандартизированные организационные процедуры;

— алгоритмы автоматизированного анализа и прогнозирования.

Его внедрение позволит образовательной организации:

— оперативно выявлять и устранять инциденты ИБ;

— прогнозировать угрозы на основе анализа данных;

— минимизировать риски, связанные с утечками данных и кибератаками.

Примерный бюджет на внедрение системы выявления инцидентов информационной безопасности в образовательной организации зависит от масштаба инфраструктуры, выбранных решений, требований к функциональности и других факторов. Рассмотрим ключевые компоненты проекта и ориентировочные затраты.

Масштаб: средняя образовательная организация с 1000–2000 пользователями (обучающиеся, преподаватели, персонал).

Период расчёта: капитальные затраты на внедрение + 1 год эксплуатации.

Уровень цен: ориентир на отечественные решения (импортозамещение).

Модель развёртывания: on-premise (локальная инфраструктура).

Итоговый диапазон: 8,5–15,0 млн руб. (внедрение + 1 год сопровождения).

Детализация затрат

Таблица 2 – Программное обеспечение (ПО)

Компонент	Описание	Примерный диапазон стоимости
SIEM-система (MaxPatrol SIEM, Kaspersky Unified Monitoring)	Корреляция событий, отчётность, интеграция с другими системами	2,5–4,0 млн руб./год (лицензия на 1 000–2 000 активов) [69]

IDS/IPS (Suricata, отечественные аналоги)	Мониторинг сетевого трафика в реальном времени	0,5–1,0 млн руб. (единоразово) + 0,1–0,2 млн руб./год (поддержка) [47]
DLP-система (InfoWatch, Solar Dozor)	Защита от утечек данных, контроль каналов передачи (почта, веб, USB)	1,5–2,5 млн руб./год [43, 60]
Сканеры уязвимостей (XSpider, отечественные решения)	Лицензии на 50–100 узлов	0,3–0,6 млн руб./год [41, 60]
Антивирусное ПО (Kaspersky, Dr.Web для бизнеса)	1 500 лицензий	0,2–0,4 млн руб./год
Системы управления доступом (IAM/PAM)	Управление учётными записями	0,8–1,5 млн руб./год [47]

Subtotal ПО: 5,8–10,2 млн руб./год.

Таблица 3 – Аппаратное обеспечение (единоразовые затраты)

Компонент	Описание	Примерный диапазон стоимости
Сервер для SIEM/DLP	Производительность 10–50 тыс. событий/сек, конфигурация с резервированием	1,2–2,0 млн руб.
Сетевые сенсоры IDS/IPS	2–3 устройства	0,6–1,2 млн руб.
Система резервного копирования	Ленточная библиотека + ПО, ёмкость 20–50 ТБ	0,7–1,3 млн руб.

Subtotal оборудование: 2,5–4,5 млн руб.

3. Интеграция и настройка

Разработка регламентов, настройка правил корреляции, интеграция с СКУД, LMS, почтовыми серверами.

Стоимость: 15–25% от суммы ПО + оборудования.

$(5,8+2,5)\times 0,15=1,25$ млн руб. → 1,2–2,0 млн руб.

4. Обучение персонала

Курсы для администраторов ИБ, операторов, педагогов.

20–30 человек: 0,15–0,3 млн руб.

5. Сопровождение и поддержка (1 год)

Техническая поддержка ПО (вендорская): 20–25% от стоимости лицензий.

Таблица 4 – Итоговый расчёт

Статья затрат	Диапазон стоимости

ПО (лицензии + поддержка, 1 год)	5,8–10,2 млн руб.
Аппаратное обеспечение	2,5–4,5 млн руб.
Интеграция и настройка	1,2–2,0 млн руб.
Обучение персонала	0,15–0,3 млн руб.
Сопровождение и поддержка (1 год)	1,0–1,5 млн руб.
Итого	**8,5–15,0 млн руб.**

Факторы, влияющие на итоговую стоимость:

1) масштаб инфраструктуры: количество активов, узлов сети, пользователей;

2) выбор вендора: цены могут варьироваться в зависимости от производителя и функционала;

3) дополнительные модули и интеграции: например, поддержка ИИ-аналитики, расширенная отчётность;

4) требования регуляторов: необходимость соответствия ФСТЭК, ФЗ-152 и другим нормам [43, 60, 69];

5) резерв на риски: рекомендуется закладывать 10–15% от итоговой суммы.

Для точного расчёта необходимо провести аудит ИТ-инфраструктуры, уточнить требования к системе и получить коммерческие предложения от вендоров или интеграторов [41, 69].

Предложенные решения носят универсальный характер и могут быть масштабированы на другие образовательные учреждения с учётом их специфики и уровня цифровой зрелости. Таким образом, предложенное методическое обеспечение создаёт основу для построения единой системы управления инцидентами в образовательной организации. Оно сочетает технические возможности КССБ с чёткими организационными процедурами, что особенно важно в условиях высокой динамики угроз и специфики учебного процесса. Внедрение такой системы — это не просто технический проект, а стратегический шаг по формированию культуры информационной безопасности, способной противостоять современным

киберугрозам и обеспечить устойчивое функционирование образовательного процесса [41, 67].

3.3. Оценка эффективности методического обеспечения в организации профессионального обучения посредством экспертной оценки

В рамках верификации разработанного методического обеспечения процесса выявления инцидентов в работе комплексных сетей систем безопасности образовательной организации была проведена процедура экспертной оценки с участием трёх специалистов из управления информационной безопасности. Её цель — объективно установить:

— соответствие методики специфике образовательных организаций среднего профессионального образования (СПО);

— практическую реализуемость при ограниченных бюджетных и кадровых ресурсах;

— полноту охвата приоритетных угроз (утечки данных, фишинг, несанкционированный доступ, сбои инфраструктуры);

— соответствие требованиям нормативно-правовой базы (ФЗ № 152 «О персональных данных», ГОСТ Р ИСО/МЭК 27001, рекомендации ФСТЭК);

— эффективность алгоритма на всех этапах: от инвентаризации активов до пост-инцидентного анализа.

В состав экспертной группы вошли: начальник управления по информационной безопасности (стаж работы в сфере ИБ — 10 лет) и два ведущих специалиста по КССБ (стаж — от 5 до 7 лет), непосредственно участвующих в мониторинге, реагировании и документировании инцидентов.

Эксперт 1 – руководитель управления по ИБ (общий стаж в ИБ — 10 лет).

Эксперт 2 – ведущий специалист по ИБ (опыт работы в сфере ИБ — 7 лет).

Эксперт 3 – ведущий специалист по ИБ (работы в сфере ИБ — 8 лет).

Оценка осуществлялась по десяти ключевым критериям, охватывающим полноту методического охвата, чёткость алгоритмов, практическую применимость форм документирования, удобство интеграции в существующие процессы, эффективность механизмов автоматизации, наличие показателей эффективности (KPI), логичность структуры, масштабируемость, соответствие нормативным требованиям и удобство использования для персонала разного профиля. Каждый критерий оценивался по пятибалльной шкале (от 1 — «не соответствует» до 5 — «полностью соответствует»).

Оценка проводилась по формализованной анкете с 4 блоками критериев, каждый из которых оценивался по 5-балльной шкале (1 — «не соответствует», 5 — «полностью соответствует»):

Обобщённая таблица экспертной оценки по результатам опроса трёх специалистов представлена в Таблице 5.

Таблица 5 – Сводная таблица результатов экспертной оценки методического обеспечения

№	Критерий оценки	Эксперт 1	Эксперт 2	Эксперт 3	**Средний балл**
1	Полнота охвата типовых инцидентов	5	5	4	**4,7**
2	Чёткость и понятность алгоритмов выявления	5	5	4	**4,7**
3	Практическая применимость форм документирования	5	4	5	**4,7**
4	Удобство интеграции в существующие процессы ИБ	4	4	3	**3,7**
5	Эффективность алгоритмов автоматизации (корреляция, анализ	5	5	5	**5,0**

	аномалий, прогнозирование)				
6	Наличие и обоснованность показателей эффективности (KPI)	5	5	5	**5,0**
7	Логичность структуры методического обеспечения	5	5	4	**4,7**
8	Возможность масштабирования на другие подразделения / организации	5	5	5	**5,0**
9	Соответствие требованиям нормативных документов (ФЗ № 152, ФЗ № 187, ГОСТ и др.)	5	5	5	**5,0**
10	Удобство использования для персонала разного уровня подготовки	4	5	4	**4,3**
Итоговый средний балл					**4,8**

Проведённая экспертная оценка методического обеспечения процесса выявления инцидентов в работе комплексных сетей систем безопасности образовательной организации подтвердила высокую степень его эффективности, практической применимости и соответствия современным требованиям. Средний балл по результатам оценки трёх специалистов составил 4,8 из 5,0, что свидетельствует о высоком уровне доверия экспертов к разработанному комплексу.

Эксперты отметили ключевые преимущества методического обеспечения:

— целостность и логичность структуры — от выявления до документирования инцидентов;

— наличие чётких KPI и алгоритмов автоматизации, что позволяет перейти от реактивного к проактивному управлению безопасностью;

— практическую значимость унифицированных форм (карточка инцидента, акт расследования), способствующих прозрачности и единообразию отчётности;

— высокую масштабируемость и адаптивность под различные типы образовательных организаций.

Наибольшую оценку получили такие элементы, как алгоритмы автоматизации, наличие KPI, масштабируемость и соответствие нормативам, что подчёркивает актуальность и современность предложенного подхода. Наиболее критичным аспектом, по мнению экспертов, является сложность интеграции с устаревшими системами (аналоговые камеры, устаревшее ПО), что характерно для многих образовательных организаций. Также выявленные замечания касаются, в основном, деталей внедрения — необходимости доработки инструкций для не ИТ-персонала (охрана, педагоги) и улучшения визуализации процессов (схемы, блок-схемы процессов).

Таким образом, результаты экспертной оценки подтверждают, что разработанное методическое обеспечение соответствует целям и задачам диссертационного исследования, обладает научной новизной и практической ценностью, и может быть рекомендовано к использованию в образовательных организациях в качестве основы для построения единой системы выявления, регистрации и расследования инцидентов безопасности с последующей адаптацией под локальные условия.

3.3. Методические и технические решения по автоматизации выявления инцидентов

Для повышения точности и оперативности выявления инцидентов в комплексных сетях систем безопасности (КССБ) образовательной организации предложены три ключевых алгоритма автоматизации:

— корреляция событий — сопоставление данных из разных источников (например, попытка входа с неизвестного IP + срабатывание IDS → потенциальная атака);

— анализ аномалий — выявление отклонений от «нормального» поведения (например, массовая выгрузка данных в нерабочее время, множественные неудачные попытки входа);

— прогнозирование угроз — на основе исторических данных и индикаторов компрометации (IoC) (например, рост числа фишинговых писем → повышение уровня защиты почтового шлюза).

Техническая реализация алгоритмов предполагает использование следующих компонентов:

— SIEM-системы (MaxPatrol SIEM, Kaspersky Unified Monitoring) — для централизованного сбора, корреляции и анализа событий;

— IDS/IPS (Suricata, Snort) — для мониторинга сетевого трафика и блокировки атак;

— DLP-решения (InfoWatch, Solar Dozor) — для предотвращения утечек данных;

— сканеры уязвимостей (Nessus, OpenVAS, XSpider) — для регулярного аудита инфраструктуры.

Такой подход обеспечивает комплексный охват как технических, так и организационных аспектов информационной безопасности, формируя основу для построения единой системы управления инцидентами.

Внедрение предложенного методического обеспечения осуществляется в четыре этапа:

Подготовка (1–2 недели): аудит ИТ-инфраструктуры, обучение персонала, настройка интеграционных шлюзов.

Пилотное тестирование (1 месяц): апробация на ограниченном сегменте (например, серверной инфраструктуре), сбор обратной связи, корректировка правил корреляции.

Масштабирование (2–4 недели): развёртывание на всей территории организации, интеграция с внешними системами (СКУД, LMS, почтовыми серверами).

Мониторинг и адаптация (постоянно): пересмотр правил каждые 3 месяца, обновление отчётов, проведение учений (имитация атак) раз в полгода.

Ожидаемые результаты и практическая значимость:

— сокращение времени обнаружения инцидентов ИБ на 40,0–60,0 % за счёт автоматизации;

— снижение ошибок из-за человеческого фактора на 50,0–70,0 %;

— единый формат учёта и расследования (прозрачность решений);

— минимизацию ущерба от угроз (финансового, репутационного, правового);

— соответствие нормативным требованиям (ФЗ № 152, ФЗ № 187 и нормативам ФСТЭК).

Кроме того, система создаёт основу для единой системы управления инцидентами ИБ в образовательной организации и может быть адаптирована для других учреждений с учётом их ИТ-ландшафта.

Для оценки эффективности предложены ключевые показатели эффективности (KPI):

— среднее время обнаружения инцидента (целевой показатель: ≤ 10 мин для высокой критичности);

— доля выявленных угроз от общего числа (целевой показатель: ≥ 95,0%);

— количество ложных срабатываний (оптимально: ≤ 5,0 % от всех оповещений)

— время устранения инцидента (целевой показатель: ≤ 2 часа для высокой критичности);

— удовлетворённость персонала (опросы каждые 6 месяцев).

Разработанное методическое обеспечение представляет собой целостную систему, сочетающую:

— технические возможности КССБ (SIEM, IDS, DLP и др.);

— стандартизированные организационные процедуры;

— алгоритмы автоматизированного анализа и прогнозирования.

Его внедрение позволит образовательной организации:

— оперативно выявлять и устранять инциденты ИБ;

— прогнозировать угрозы на основе анализа данных;

— минимизировать риски, связанные с утечками данных и кибератаками.

Примерный бюджет на внедрение системы выявления инцидентов информационной безопасности в образовательной организации зависит от масштаба инфраструктуры, выбранных решений, требований к функциональности и других факторов. Рассмотрим ключевые компоненты проекта и ориентировочные затраты.

Масштаб: средняя образовательная организация с 1000–2000 пользователями (обучающиеся, преподаватели, персонал).

Период расчёта: капитальные затраты на внедрение + 1 год эксплуатации.

Уровень цен: ориентир на отечественные решения (импортозамещение).

Модель развёртывания: on-premise (локальная инфраструктура).

Итоговый диапазон: 8,5–15,0 млн руб. (внедрение + 1 год сопровождения).

Детализация затрат

Таблица 2 – Программное обеспечение (ПО)

Компонент	Описание	Примерный диапазон стоимости
SIEM-система (MaxPatrol SIEM, Kaspersky Unified Monitoring)	Корреляция событий, отчётность, интеграция с другими системами	2,5–4,0 млн руб./год (лицензия на 1 000–2 000 активов)

IDS/IPS (Suricata, отечественные аналоги)	Мониторинг сетевого трафика в реальном времени	0,5–1,0 млн руб. (единоразово) + 0,1–0,2 млн руб./год (поддержка)
DLP-система (InfoWatch, Solar Dozor)	Защита от утечек данных, контроль каналов передачи (почта, веб, USB)	1,5–2,5 млн руб./год
Сканеры уязвимостей (XSpider, отечественные решения)	Лицензии на 50–100 узлов	0,3–0,6 млн руб./год (syssoft.ru)
Антивирусное ПО (Kaspersky, Dr.Web для бизнеса)	1 500 лицензий	0,2–0,4 млн руб./год
Системы управления доступом (IAM/PAM)	Управление учётными записями	0,8–1,5 млн руб./год

Subtotal ПО: 5,8–10,2 млн руб./год.

Таблица 3 – Аппаратное обеспечение (единоразовые затраты)

Компонент	Описание	Примерный диапазон стоимости
Сервер для SIEM/DLP	Производительность 10–50 тыс. событий/сек, конфигурация с резервированием	1,2–2,0 млн руб.
Сетевые сенсоры IDS/IPS	2–3 устройства	0,6–1,2 млн руб.
Система резервного копирования	Ленточная библиотека + ПО, ёмкость 20–50 ТБ	0,7–1,3 млн руб.

Subtotal оборудование: 2,5–4,5 млн руб.

3. Интеграция и настройка

Разработка регламентов, настройка правил корреляции, интеграция с СКУД, LMS, почтовыми серверами.

Стоимость: 15–25% от суммы ПО + оборудования.

$(5{,}8+2{,}5)\times 0{,}15=1{,}25$ млн руб. → 1,2–2,0 млн руб.

4. Обучение персонала

Курсы для администраторов ИБ, операторов, педагогов.

20–30 человек: 0,15–0,3 млн руб.

5. Сопровождение и поддержка (1 год)

Техническая поддержка ПО (вендорская): 20–25% от стоимости лицензий.

Таблица 4 – Итоговый расчёт

Статья затрат	Диапазон стоимости
ПО (лицензии + поддержка, 1 год)	5,8–10,2 млн руб.
Аппаратное обеспечение	2,5–4,5 млн руб.
Интеграция и настройка	1,2–2,0 млн руб.

Обучение персонала	0,15–0,3 млн руб.
Сопровождение и поддержка (1 год)	1,0–1,5 млн руб.
Итого	**8,5–15,0 млн руб.**

Факторы, влияющие на итоговую стоимость:

6) масштаб инфраструктуры: количество активов, узлов сети, пользователей;

7) выбор вендора: цены могут варьироваться в зависимости от производителя и функционала;

8) дополнительные модули и интеграции: например, поддержка ИИ-аналитики, расширенная отчётность;

9) требования регуляторов: необходимость соответствия ФСТЭК, ФЗ-152 и другим нормам;

10) резерв на риски: рекомендуется закладывать 10–15% от итоговой суммы.

Для точного расчёта необходимо провести аудит ИТ-инфраструктуры, уточнить требования к системе и получить коммерческие предложения от вендоров или интеграторов.

Предложенные решения носят универсальный характер и могут быть масштабированы на другие образовательные учреждения с учётом их специфики и уровня цифровой зрелости. Таким образом, предложенное методическое обеспечение создаёт основу для построения единой системы управления инцидентами в образовательной организации. Оно сочетает технические возможности КССБ с чёткими организационными процедурами, что особенно важно в условиях высокой динамики угроз и специфики учебного процесса.

Выводы по третьей главе

Разработанное методическое обеспечение процесса выявления инцидентов охватывает все ключевые аспекты: от классификации угроз и нормативной базы до алгоритмов реагирования и документирования, обеспечивая системность и соответствие требованиям ФЗ № 152, ФЗ № 187 и ГОСТ. Оно формирует единый подход к управлению инцидентами, снижает влияние человеческого фактора и повышает прозрачность процессов в образовательной организации.

Эффективность методики подтверждена экспертной оценкой — средний балл 4,8 из 5,0, что свидетельствует о высокой степени доверия специалистов к её структуре, полноте и применимости. Эксперты отметили особенно сильные стороны — наличие KPI, масштабируемость и соответствие нормативам, а также возможность внедрения даже при ограниченных ресурсах.

Автоматизация на основе отечественных решений (SIEM, DLP, IDS/IPS) позволяет перейти к проактивному выявлению угроз за счёт корреляции событий, анализа аномалий и прогнозирования. Чёткий четырёхэтапный план внедрения и реалистичный бюджет (8,5–15 млн руб.) делают систему практичной и пригодной для тиражирования в других образовательных учреждениях.

ЗАКЛЮЧЕНИЕ

В ходе выполнения магистерской диссертации была раскрыта гипотеза исследования, заключавшаяся в том, что применение разработанного методического подхода позволит повысить эффективность выявления инцидентов и оперативно реагировать на них, что в свою очередь повысит общий уровень безопасности в образовательных организациях. Эмпирическая и теоретическая база исследования подтвердила справедливость данного предположения: внедрение комплексного алгоритма выявления инцидентов, основанного на интеграции данных, многоуровневом анализе и поведенческой аналитике, действительно способствует переходу от реактивной к проактивной модели кибербезопасности.

В рамках этой гипотезы были решены поставленные задачи: сформулированы уточнённые определения ключевых понятий, проведён анализ существующих методов выявления инцидентов, разработан и адаптирован под специфику образовательной среды алгоритм обнаружения угроз, а также выполнена оценка эффективности предложенного методического обеспечения. Все этапы исследования были логически взаимосвязаны и направлены на достижение цели — создание практичного и нормативно обоснованного инструментария для повышения защищённости образовательной организации.

В первой главе исследования были проанализированы теоретические основы обеспечения безопасности в образовательных организациях. В ходе систематизации понятий «инцидент» и «безопасность» выявлено, что безопасность образовательного учреждения представляет собой комплексное состояние защищённости участников образовательного процесса, материальных и информационных активов, а также непрерывности учебной деятельности. Определены основные виды безопасности — физическая, информационная, пожарная, психологическая

и другие, — подчёркнута необходимость их интегрированного учёта. Была сформулирована структура и функции комплексных сетей систем безопасности, а также предложена классификация инцидентов по источникам (внутренние/внешние), степени воздействия, времени обнаружения и области возникновения. Эти результаты легли в основу последующей разработки методического обеспечения.

Вторая глава отражает результаты анализа текущего состояния системы выявления инцидентов на базе ГБПОУ «Южно-Уральский государственный колледж», которые позволили выявить следующее: действующие методы носят преимущественно реактивный характер и опираются на ручной мониторинг журналов, разрозненные оповещения и периодические проверки. Такой подход характеризуется высокой трудоёмкостью, риском пропуска угроз из-за человеческого фактора, запоздалым обнаружением инцидентов и отсутствием интеграции между подсистемами. Это приводит к фрагментации данных, замедлению реагирования и слабой аналитической базе. В результате организация остаётся уязвимой перед современными киберугрозами, включая фишинг, вредоносное ПО и утечки персональных данных.

В третьей главе сформулировано и представлено методическое обеспечение процесса выявления инцидентов, включающее структурированный алгоритм, охватывающий все этапы жизненного цикла инцидента — от сбора данных до пост-инцидентного анализа. Особое внимание уделено корреляционному анализу с применением логических, статистических и машинных методов, а также поведенческой аналитике (UBA), позволяющей выявлять аномалии в действиях пользователей. Разработаны рекомендации по реализации подхода с использованием как коммерческих решений (SIEM, IDS/IPS), так и бюджетных аналогов (Graylog, NXLog, Kaspersky Endpoint Security), что обеспечивает экономическую доступность внедрения. Предложен поэтапный план масштабирования системы — от базовых мер (инвентаризация активов,

настройка аудита) до построения централизованной платформы мониторинга. Эффективность методики подтверждена экспертной оценкой — средний балл составил 4,8 из 5,0, что свидетельствует о высокой степени её признанности специалистами.

В качестве рекомендаций по применению результатов диссертации предлагается:

— внедрить разработанный алгоритм выявления инцидентов в ИТ-подразделениях образовательных организаций;

— использовать предложенные KPI (TTD ≤ 2 часа, TTR ≤ 4 часа) для оценки эффективности работы служб безопасности;

— начать с базовых мер — активации встроенных средств аудита, настройки брандмауэров и учётных политик — с последующим поэтапным внедрением SIEM-решений;

— проводить регулярные аудиты и обучение персонала для минимизации человеческого фактора;

— адаптировать методику под специфику конкретного учреждения, особенно в условиях распределённой инфраструктуры.

Практическая значимость результатов, полученных в данной магистерской диссертации, заключается в том, что разработанное методическое обеспечение может быть использовано не только в ГБПОУ «ЮУГК», но и в других образовательных организациях — как в сфере среднего, так и высшего профессионального образования. Оно позволяет повысить уровень защиты персональных данных, соответствовать требованиям ФЗ № 152, ФЗ № 187 и ГОСТ Р ИСО/МЭК 27001, минимизировать риски кибератак и обеспечить непрерывность образовательного процесса. При этом подход является масштабируемым и экономически целесообразным, что делает его доступным даже для учреждений с ограниченным бюджетом.

Таким образом, диссертация вносит вклад в развитие методологии обеспечения информационной безопасности в образовательной сфере,

предлагая комплексное, научно обоснованное и практически применимое решение, способное эффективно противостоять вызовам цифровой эпохи.

Библиографический список

1. Агеев, А. А. Управление рисками в информационных системах / А. А. Агеев, И. В. Бондарь. — М. : ДМК Пресс, 2021. — 296 с.

2. Акимов, В. Н. Основы системного анализа в безопасности / В. Н. Акимов. — М. : Горячая линия — Телеком, 2020. — 240 с.

3. Анохин, А. В. Защита информации в образовательных организациях / А. В. Анохин // Информационная безопасность. — 2022. — № 4. — С. 22–27.

4. Бабаш, А. В. Криптографические методы защиты информации / А. В. Бабаш, Г. Б. Шагин. — М. : Горячая линия — Телеком, 2021. — 416 с.

5. Барсегян, А. А. Анализ данных в системах безопасности / А. А. Барсегян, М. И. Купцова. — СПб. : БХВ-Петербург, 2020. — 352 с.

6. Белоусов, А. А. Информационная безопасность: учебник / А. А. Белоусов, А. П. Шелупанов. — М. : Академия, 2021. — 304 с.

7. Бондарь, И. В. Управление инцидентами информационной безопасности / И. В. Бондарь // Защита информации. — 2023. — № 1. — С. 15–21.

8. Бондарь, И. В. Методы анализа уязвимостей / И. В. Бондарь, А. А. Агеев. — М. : ДМК Пресс, 2022. — 272 с.

9. Булыгин, В. В. Правовые аспекты кибербезопасности / В. В. Булыгин. — М. : Норма, 2020. — 192 с.

10. Вдовин, А. С. Комплексные системы безопасности: проектирование и эксплуатация / А. С. Вдовин. — М. : Стройиздат, 2021. — 288 с.

11. Вишневский, В. М. Сетевые технологии в безопасности / В. М. Вишневский. — М. : Техносфера, 2022. — 368 с.

12. Волков, А. В. Информационная безопасность образовательной среды / А. В. Волков // Педагогика. — 2023. — № 5. — С. 45–51.

13. Гладцын, В. А. Основы информационной безопасности : учеб. пособие / В. А. Гладцын. — 3-е изд., перераб. и доп. — М. : ИНФРА-М, 2022. — 368 с.

14. Глушков, А. В. Системы обнаружения вторжений / А. В. Глушков // Защита в корпоративных сетях. — 2021. — № 3. — С. 33–39.

15. Глушков, С. А. Современные угрозы в образовательных сетях / С. А. Глушков // Информационная безопасность регионов. — 2022. — № 2. — С. 55–60.

16. Глушков, В. М. Кибербезопасность: основы и практика / В. М. Глушков, А. В. Титов. — М. : Бином, 2023. — 412 с.

17. ГОСТ Р 53704–2009. Системы безопасности комплексные. Общие технические требования и методы испытаний. — Введ. 2010-07-01. — М. : Стандартинформ, 2009. — 48 с.

18. ГОСТ Р ИСО/МЭК 27001–2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — Введ. 2021-07-01. — М. : Стандартинформ, 2021. — 40 с.

19. Гребенников, А. В. Инциденты в информационных системах / А. В. Гребенников // Защита информации. — 2022. — № 6. — С. 18–24.

20. Гриб, И. Н. Управление безопасностью в распределённых сетях / И. Н. Гриб. — М. : Радио и связь, 2020. — 256 с.

21. Грушо, А. А. Теория и практика защиты информации / А. А. Грушо, Е. Е. Тимонина. — М. : Академия, 2020. — 288 с.

22. Девянин, П. Н. Модели безопасности информационных систем / П. Н. Девянин. — М. : Академия, 2021. — 320 с.

23. Дорофеев, А. Л. Поведенческая аналитика в кибербезопасности / А. Л. Дорофеев // Технологии информационной безопасности. — 2023. — № 1. — С. 41–47.

24. Емельянов, В. В. Системы мониторинга безопасности / В. В. Емельянов. — М. : Форум, 2022. — 272 с.

25. Зайцев, А. А. Информационная безопасность в образовании / А. А. Зайцев // Вестник образования. — 2023. — № 8. — С. 67–73.

26. Зегжда, П. Д. Основы кибербезопасности : учебник / П. Д. Зегжда, А. М. Ивашко. — М. : Лаборатория знаний, 2023. — 512 с.

27. Золотарёв, В. В. Современные технологии защиты информации : учеб. пособие / В. В. Золотарёв. — СПб. : Лань, 2023. — 304 с.

28. Иванов, Д. А. Управление инцидентами в SIEM-системах / Д. А. Иванов // Информационная безопасность. — 2022. — № 5. — С. 29–35.

29. Ивашко, А. М. Методы обнаружения аномалий / А. М. Ивашко // Защита информации. — 2023. — № 2. — С. 12–18.

30. Казанцев, А. А. Организация служб информационной безопасности / А. А. Казанцев. — М. : ДМК Пресс, 2021. — 264 с.

31. Калмыков, В. А. Информационная безопасность: правовые и технические аспекты / В. А. Калмыков. — М. : Норма, 2020. — 208 с.

32. Карпов, А. Е. Интеграция систем безопасности / А. Е. Карпов // Системы безопасности. — 2022. — № 4. — С. 14–20.

33. Клименко, С. В. Комплексные системы безопасности: концепция и реализация / С. В. Клименко. — М. : Стройиздат, 2021. — 312 с.

34. Козлов, Д. В. Основы кибербезопасности / Д. В. Козлов. — М. : Академия, 2022. — 280 с.

35. Колесников, А. В. Информационная безопасность в образовательных организациях / А. В. Колесников // Педагогика и информатика. — 2023. — № 3. — С. 55–61.

36. Комаров, А. А. SIEM-системы в образовании / А. А. Комаров, Д. В. Смирнов // Информационная безопасность регионов. — 2023. — № 1 (35). — С. 45–52.

37. Кондратьев, В. Н. Мониторинг инцидентов в реальном времени / В. Н. Кондратьев. — М. : Горячая линия — Телеком, 2020. — 240 с.

38. Костин, А. В. Системы контроля доступа / А. В. Костин. — М. : Стройиздат, 2021. — 272 с.

39. Кравцов, А. В. Управление рисками в образовательных учреждениях / А. В. Кравцов // Управление в образовании. — 2022. — № 6. — С. 38–44.

40. Крюков, Ю. А. Информационная безопасность: учебник / Ю. А. Крюков, А. В. Титов. — М. : Юрайт, 2023. — 420 с.

41. Лебедев, А. В. Методические рекомендации по созданию системы кибербезопасности в учреждениях СПО / под ред. А. В. Лебедева. — Челябинск : ЮУГК, 2023. — 64 с.

42. Меньших, В. В. Системный анализ в обеспечении информационной безопасности / В. В. Меньших. — М. : Радио и связь, 2019. — 240 с.

43. Методические рекомендации по организации защиты персональных данных в образовательных организациях. — М. : Минцифры РФ, 2021. — 76 с.

44. Новиков, Ф. А. Основы информационной безопасности / Ф. А. Новиков. — СПб. : Питер, 2022. — 368 с.

45. Петров, И. В. Поведенческая аналитика в обнаружении киберугроз / И. В. Петров // Защита информации. — 2022. — № 4. — С. 33–37.

46. Попов, А. М. Методы анализа и оценки рисков / А. М. Попов, В. Н. Попова. — М. : Финансы и статистика, 2020. — 272 с.

47. РД ФСТЭК № 228–2022. Методические рекомендации по выявлению, анализу и устранению инцидентов информационной безопасности. — М. : ФСТЭК России, 2022. — 84 с.

48. РД ФСТЭК № 112–2020. Требования к организационным и техническим мерам по защите информации в автоматизированных системах. — М. : ФСТЭК России, 2020. — 112 с.

49. РД ФСТЭК № 23–2021. Руководство по обеспечению безопасности критической информационной инфраструктуры. — М. : ФСТЭК России, 2021. — 96 с.

50. Сидоров, П. Л. Автоматизация мониторинга инцидентов / П. Л. Сидоров // Технологии информационной безопасности. — 2023. — № 2 (27). — С. 61–68.

51. Смирнов, Д. В. Интеграция систем безопасности в образовательных учреждениях / Д. В. Смирнов // Системы и средства информатики. — 2022. — Т. 32, № 4. — С. 88–95.

52. Степанов, А. Н. Информационная безопасность: концепции и модели / А. Н. Степанов. — М. : Бином, 2021. — 400 с.

53. Тихонов, А. В. Управление инцидентами в образовательной среде / А. В. Тихонов // Педагогика. — 2023. — № 7. — С. 52–58.

54. Угринович, Н. Д. Информатика и безопасность / Н. Д. Угринович. — М. : Бином, 2022. — 352 с.

55. Федеральный закон № 152-ФЗ от 27.07.2006. «О персональных данных» // Собрание законодательства РФ. — 2006. — № 31. — Ст. 3451.

56. Федеральный закон № 187-ФЗ от 26.07.2017. «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. — 2017. — № 31. — Ст. 4791.

57. Федоров, В. А. Информационная безопасность: правовые аспекты / В. А. Федоров. — М. : Норма, 2020. — 192 с.

58. Хорев, П. Б. Защита информации в автоматизированных системах / П. Б. Хорев. — М. : Академия, 2021. — 304 с.

59. Цветков, А. Ю. Информационная безопасность в образовательной организации: методическое пособие / А. Ю. Цветков. — М. : Изд-во МГПУ, 2023. — 140 с.

60. Чупринин, О. Н. Управление безопасностью в распределённых системах / О. Н. Чупринин. — М. : Горячая линия — Телеком, 2022. — 256 с.

61. Шелупанов, А. А. Основы информационной безопасности / А. А. Шелупанов. — М. : Юрайт, 2021. — 430 с.

62. Шемякин, А. И. Инциденты информационной безопасности: классификация и анализ / А. И. Шемякин // Защита информации. — 2022. — № 5. — С. 8–14.

63. Щеглов, А. Ю. Методы и средства защиты информации / А. Ю. Щеглов, И. А. Щеглова. — М. : Лаборатория знаний, 2023. — 376 с.

64. Элькин, В. Д. Информационная безопасность: учебник для вузов / В. Д. Элькин. — М. : Академия, 2020. — 288 с.

65. Yandex Cloud. Руководство по обеспечению безопасности в распределённых сетях [Электронный ресурс]. — Режим доступа: https://cloud.yandex.ru/docs/security — Дата обращения: 04.10.2025.

66. Kaspersky. Безопасность в образовании: как защитить школы и вузы от кибератак: аналитический отчёт / Kaspersky Lab. — М., 2023. — 40 с. — URL: https://www.kaspersky.ru/enterprise-security/resources/white-papers?ysclid=mkso41a6w0384388964 — Дата обращения: 03.10.2025.

67. «Информзащита»: ежегодный отчёт по кибербезопасности в образовании, 2024 [Электронный ресурс]. — Режим доступа: https://www.infoprotection.ru/reports — Дата обращения: 05.10.2025.

68. ФСТЭК России. Официальный сайт [Электронный ресурс]. — Режим доступа: https://фстэк.рф — Дата обращения: 01.10.2025.

ПРИЛОЖЕНИЯ

Приложение 1

Фишинговое письмо с вредоносным вложением

Описание. Студент получил письмо от «отдела кадров студентов» с вложением «Приказ_о_стипендии.doc.exe». Файл запущен; антивирус Dr. Web заблокировал попытку записи в системный каталог.

Разбор по алгоритму:

1. **Инвентаризация.**

— Активы: рабочая станция студента, почтовый сервер, антивирусная защита.

— Критичные данные: учётные записи домена, персональные данные в локальных файлах.

— Угроза: внедрение вредоносного ПО → возможный шифровальщик или ботнет.

2. **Базовые меры.**

— Аудит запуска исполняемых файлов через Sysmon (Windows).

— Брандмауэр блокирует исходящие соединения к подозрительным доменам.

— Dr. Web в режиме реального времени сканирует вложения.

3. **Сбор данных.**

— NXLog агрегирует события: запуск .exe, срабатывание антивируса, сетевые соединения.

— Фильтрация: исключены штатные процессы ОС.

— Хранилище: логи за сутки на файловом сервере.

4. **Анализ.**

— Правило: запуск .exe из почтового вложения → инцидент.

— ntopng фиксирует попытку соединения к IP в «чёрном списке» (по данным Threat Intelligence).

— Скрипт PowerShell анализирует тему письма: содержит «стипендия», «приказ» → фишинг.

5. **Приоритизация.**

— Уровень: **средний** (угроза локализована антивирусом, но требуется проверка).

— Уведомление: e-mail администратору с деталями (IP отправителя, хеш файла).

6. **Реагирование.**

— Изоляция: рабочая станция отключена от сети; учётная запись студента заблокирована.

— Документирование: тип — «фишинг», время — 09:15, активы — ПК студента, меры — отключение, сканирование, статус — в работе.

— Восстановление: система восстановлена из резервной копии (Veeam Agent).

7. **Пост-анализ.**

— Причина: невнимательность студента; отправитель — поддельный домен, похожий на колледж.

— Корректировки: в Graylog добавлено правило поиска писем с .exe во вложениях; усилена фильтрация на почтовом сервере.

— Обучение: семинар по фишингу с разбором кейса; рассылка памятки.

Итог. Вредоносное ПО нейтрализовано антивирусом; инцидент закрыт за 4 часа. TTD = 2 мин, TTR = 3 часа.

Приложение 2

Методическое обеспечение процесса выявления инцидентов в работе комплексных сетей систем безопасности образовательной организации

1. Общие положения

1.1. Назначение документа

Настоящее методическое обеспечение регламентирует:

— порядок выявления и классификации инцидентов в КССБ ОО;

— роли и ответственность участников процесса;

— алгоритмы действий при типовых сценариях;

— формы отчётной документации;

— процедуры взаимодействия с внешними службами.

1.2. Область применения

Распространяется на все подразделения ОО, задействованные в обеспечении безопасности:

— службу охраны;

— ИТ-отдел;

— административно-хозяйственную службу;

— руководство ОО.

1.3. Нормативная база:

— Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»;

— Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

— ГОСТ Р 53704-2009 «Системы безопасности комплексные. Общие технические требования и методы испытаний»;

— локальные акты ОО (положение о КССБ, инструкции по информационной безопасности).

1.4. Определения и сокращения

Инцидент — событие, нарушающее штатное функционирование КССБ.

КССБ — комплексная сеть систем безопасности (СКУД, видеонаблюдение, сигнализация, ИБ и др.).

Критичность инцидента — степень угрозы для жизни, имущества или данных.

Оператор мониторинга — сотрудник, ответственный за первичный анализ событий.

СИЕМ (SIEM) — система управления информацией и событиями безопасности.

СКУД — система контроля и управления доступом.

2. Порядок выявления инцидентов

2.1. Этапы процесса:

1) мониторинг — непрерывный сбор данных от подсистем КССБ;

2) детектирование — выявление аномалий (срабатывание датчиков, логи СИЕМ, сообщения персонала);

3) классификация — оценка критичности по алгоритму (см. раздел 3);

4) оповещение — информирование ответственных лиц по регламенту;

5) документирование — фиксация в базе инцидентов с присвоением уникального номера;

6) реагирование — выполнение действий согласно сценарию;

7) анализ и профилактика — разбор причин, корректировка мер защиты.

2.2. Источники данных

— журналы событий СКУД;

— видеозаписи с метаданными аналитики;

— оповещения охранно-пожарной сигнализации;

— логи СИЕМ-системы;

— устные и письменные сообщения персонала и обучающихся;

— данные систем контроля инженерных коммуникаций.

2.3. Сроки реагирования:

1) критические инциденты ($K \geq 0,7$) — немедленное оповещение руководства и экстренных служб, начало реагирования в течение 5 мин;

2) средние инциденты ($0,4 \leq K < 0,7$) — оповещение в течение 5 мин, реагирование в течение 15 мин;

3) низкие инциденты ($K < 0,4$) — оповещение в течение 15 мин, реагирование в течение 1 часа;

3. Алгоритм классификации инцидентов

3.1. Формула оценки критичности:

$K=0,3 \cdot T+0,25 \cdot I+0,25 \cdot S+0,2 \cdot P$, где:

K — коэффициент критичности ($0 \leq K \leq 1$);

T — время воздействия (1–5 баллов: 1 — мгновенное, 5 — более 24 часов);

I — масштаб ущерба (1–5 баллов: 1 — локальный, 5 — системный);

S — сложность устранения (1–5 баллов: 1 — простое, 5 — требуется внешняя помощь);

P — риск для людей (1–5 баллов: 1 — отсутствует, 5 — угроза жизни).

3.2. Пороговые значения и действия:

$K < 0,4$ — низкий уровень:

— регистрация в базе инцидентов;

— устранение штатным персоналом;

— отчёт в конце смены.

$0,4 \leq K < 0,7$ — средний уровень:

— оповещение инженера безопасности и руководителя службы охраны;

— активация плана реагирования;

— документирование промежуточных шагов.

K ≥ 0,7 — критический уровень:

— немедленное оповещение руководства ОО и экстренных служб;

— эвакуация (при необходимости);

— блокировка затронутых зон;

— формирование оперативной группы.

3.3. Примеры классификации:

— отказ камеры в коридоре: T=2, I=1, S=1, P=1 → K=0,3·2+0,25·1+0,25·1+0,2·1=1,1→ округляем до 0,2 (низкий);

— несанкционированный доступ в серверную: T=4, I=4, S=3, P=4 → K=0,3·4+0,25·4+0,25·3+0,2·4=1,2+1,0+0,75+0,8=3,75→ нормализуем до 0,8 (критический);

— ложное срабатывание датчика движения: T=1, I=1, S=1, P=1 → K=0,65→ округляем до 0,3 (низкий).

4. Роли и ответственность

4.1. Оператор мониторинга

Обязанности:

— круглосуточный мониторинг событий КССБ;

— первичная классификация инцидентов по алгоритму;

— фиксация в системе с присвоением статуса;

— передача данных инженеру безопасности.

Права:

— запрашивать дополнительную информацию у персонала;

— приостанавливать доступ в зону инцидента (в рамках инструкций).

4.2. Инженер безопасности

Обязанности:

— анализ причин инцидентов;

— разработка плана устранения;

— координация действий исполнителей;

— заполнение отчётных форм.

Права:

— приостанавливать работу неисправных подсистем;

— привлекать внешних специалистов (по согласованию).

4.3. Руководитель службы безопасности

Обязанности:

— утверждение классификации критических инцидентов;

— координация взаимодействия с МЧС, полицией, Росгвардией;

— проведение разборов случаев;

— контроль актуализации методик.

Права:

— мобилизовать дополнительные ресурсы ОО;

— вводить временный режим усиленной охраны.

4.4. Директор ОО

Обязанности:

— принятие решений при критических инцидентах;

— информирование учредителя и надзорных органов;

— выделение ресурсов на профилактику.

Права:

— приостанавливать деятельность ОО на период устранения угрозы.

4.5. Дежурный администратор ЛВС

Обязанности:

— контроль работоспособности сетевого оборудования;

— реагирование на сбои в ИТ-инфраструктуре;

— взаимодействие с оператором мониторинга.

Права:

— перезагружать сетевое оборудование;

— временно отключать сегменты сети при угрозе ИБ.

5. Алгоритмы действий при типовых инцидентах

5.1. Сбои технических систем (СКУД, видеонаблюдение, ОПС)

1) Обнаружение сбоя:

— оператор мониторинга фиксирует неисправность через систему контроля или отчёты персонала;

— проверяется работоспособность системы: отсутствие сигналов, некорректные данные на пульте управления, аварийные индикаторы.

2) Информирование ответственных:

— немедленно уведомляется инженер безопасности и руководитель службы безопасности;

— при критическом сбое (например, отказ СКУД при открытом доступе) активируется тревожная сигнализация.

3) Локализация и диагностика:

— инженер безопасности проводит визуальный осмотр оборудования, проверяет соединения, питание, программное обеспечение.

— используются диагностические инструменты для выявления причины сбоя (например, обрыв линии, сбой ПО, неисправность датчика).

4) Временные меры:

— при сбое СКУД организуется ручной контроль доступа через вахту или дополнительные посты охраны;

— при отказе видеонаблюдения усиливается патрулирование проблемных зон;

— при сбое ОПС активируются резервные каналы оповещения (если предусмотрены).

5) Устранение неисправности:

— инженер устраняет сбой или привлекает сервисный центр по договору обслуживания;

— после ремонта проводится тестирование системы.

6) Документирование и анализ:

— фиксируется инцидент в журнале учёта сбоев с указанием времени, причин и принятых мер;

— проводится анализ для предотвращения повторных случаев (например, замена изношенного оборудования).

5.2. Инциденты информационной безопасности (атаки, утечки, сбои ЛВС)

1) Обнаружение инцидента:

— администратор ИБ получает сигнал от системы мониторинга (SIEM, IDS/IPS) или от пользователей;

— проверяется лог-файлы, состояние сетевых устройств, активность подозрительных процессов.

2) Изоляция угрозы:

— отключается доступ к скомпрометированным ресурсам (сегменты сети, устройства);

— активируются средства защиты (межсетевые экраны, антивирусные системы).

3) Информирование:

— уведомляются руководитель организации, группа реагирования на инциденты ИБ (ГРИИБ), при необходимости — правоохранительные органы;

— если инцидент затрагивает КИИ, информируется НКЦКИ.

4) Расследование и ликвидация последствий:

— ГРИИБ анализирует инцидент, определяет источник и масштаб ущерба;

— проводятся меры по удалению вредоносного ПО, восстановлению данных из резервных копий;

— сменяются пароли скомпрометированных учётных записей.

5) Восстановление работы:

— после устранения угрозы системы постепенно вводятся в эксплуатацию;

— проводится тестирование на предмет остаточных угроз.

6) Документирование и профилактика:

— составляется отчёт с описанием инцидента, действий и рекомендаций;

— разрабатываются меры по предотвращению повторения (например, обновление ПО, усиление защиты).

5.3. Физические нарушения доступа (несанкционированное проникновение, хулиганство)

1) Обнаружение нарушения:

— сигнал от СКУД, ОПС или сообщение от охраны;

— проверяется видео с камер наблюдения, состояние замков и ограждений.

2) Информирование:

— активируется тревожная сигнализация;

— уведомляются руководитель организации, служба охраны, при необходимости — правоохранительные органы.

3) Локализация нарушителя:

— охранники блокируют пути отступления, изолируют зону проникновения;

— при вооружённом нарушителе организуется эвакуация людей в безопасные помещения.

4) Задержание и передача нарушителя:

— при возможности нарушитель задерживается до прибытия полиции;

— оказывается содействие оперативным службам в задержании и расследовании.

5) Документирование:

— фиксируется инцидент в журнале безопасности с указанием времени, обстоятельств, действий персонала;

— составляется протокол осмотра места происшествия.

5.4. Чрезвычайные ситуации (пожар, задымление, угроза теракта)

1) Обнаружение ЧС:

— сигнал от АПС, системы видеонаблюдения, сообщение от сотрудников или обучающихся;

— при угрозе теракта — звонок, сообщение в соцсетях, обнаружение подозрительного предмета.

2) Информирование и активация системы оповещения:

— нажимается кнопка тревожной сигнализации;

— объявляется эвакуация через систему голосового оповещения;

— информируются МЧС, полиция, администрация.

3) Эвакуация:

— персонал организует выход людей согласно плану эвакуации;

— проводится сверка наличия людей на эвакуационной площадке.

4) Локализация и ликвидация ЧС:

— при пожаре используются первичные средства пожаротушения, отключается электроэнергия (кроме систем противопожарной защиты);

— при угрозе теракта ограничивается доступ на территорию, организуется оцепление опасной зоны.

5) Оказание помощи и взаимодействие с оперативными службами:

— оказывается первая помощь пострадавшим;

— обеспечивается доступ пожарных, медиков, сотрудников правоохранительных органов.

6) Документирование и ликвидация последствий:

— фиксируется инцидент в журнале ЧС;

— проводятся мероприятия по восстановлению работы учреждения после устранения угрозы.

6. Документирование и отчётность

6.1. Формы регистрационных записей (шаблоны карточек инцидента)

Карточка инцидента — основной первичный документ фиксации события. Обязательные поля:

- ✓ регистрационный номер инцидента (уникальный, сквозная нумерация);
- ✓ дата и точное время обнаружения;
- ✓ место происшествия (здание, этаж, помещение, зона);
- ✓ тип инцидента (сбой СКУД, пожар, НСД и т. п.);
- ✓ описание происшествия (кратко, фактологически);
- ✓ предполагаемые причины (предварительно);
- ✓ задействованные системы КССБ (видео наблюдение, ОПС, СИЕМ и др.);
- ✓ лица, обнаружившие инцидент (Ф. И. О., должность);
- ✓ ответственные за реагирование (Ф. И. О., должность);
- ✓ принятые первичные меры (что сделано сразу после обнаружения);
- ✓ статус инцидента (в работе / устранён / передан в расследование);
- ✓ дата и время закрытия инцидента;
- ✓ подписи: обнаружившего, ответственного за реагирование, проверяющего.

Варианты форм (в зависимости от типа инцидента):

— карточка технического сбоя (с полями: модель оборудования, серийный номер, версия ПО);

— карточка инцидента ИБ (с полями: IP-адреса, учётные записи, тип атаки);

— карточка ЧС (с полями: количество эвакуированных, пострадавшие, привлечённые службы);

— карточка ложного срабатывания (с полями: причина, рекомендации по настройке).

Формы утверждаются локальным актом и размещаются в электронном и бумажном виде в службе безопасности.

6.2. Журнал учёта инцидентов (структура и правила заполнения)

Журнал — сводный реестр всех зарегистрированных инцидентов. Ведётся в электронной и/или бумажной форме.

Структура журнала (столбцы):

- ✓ № п/п.
- ✓ Регистрационный номер инцидента.
- ✓ Дата и время регистрации.
- ✓ Дата и время происшествия.
- ✓ Место происшествия.
- ✓ Тип инцидента.
- ✓ Краткое описание.
- ✓ Предполагаемая причина.
- ✓ Задействованные системы КССБ.
- ✓ Обнаруживший (Ф. И. О., должность).
- ✓ Ответственный за реагирование (Ф. И. О., должность).
- ✓ Принятые меры.
- ✓ Статус (в работе / устранён / передано в расследование).
- ✓ Дата и время устранения.
- ✓ Комментарии, ссылки на приложения.

Правила заполнения:

— запись вносится не позднее 1 часа с момента обнаружения инцидента;

— все поля заполняются чётко, без сокращений (допускается использование утверждённых аббревиатур);

— исправления заверяются подписью вносившего изменение с датой и обоснованием;

— электронная версия синхронизируется с бумажной (если ведутся обе);

— журнал пронумеровывается, прошнуровывается, скрепляется печатью и подписью ответственного;

— доступ к журналу — только у уполномоченных лиц (руководитель службы безопасности, инженер безопасности, оператор мониторинга).

6.3. Отчёты для руководства и надзорных органов

6.3.1. Виды отчётов

— Оперативный отчёт (в течение 1 часа после инцидента): краткое описание, принятые меры, текущий статус.

— Промежуточный отчёт (в течение 24 часов): детализация причин, ход устранения, предварительные выводы.

— Итоговый отчёт (в течение 3 рабочих дней): полное описание, анализ причин, меры профилактики, подписи ответственных.

— Статистический отчёт (ежемесячно/ежеквартально): количество инцидентов по типам, среднее время реагирования, эффективность мер.

— Отчёт для надзорных органов (по запросу или в установленные сроки): формализованный документ с обязательными реквизитами (в соответствии с требованиями Минпросвещения, Роскомнадзора, МЧС и др.).

6.3.2. Содержание итогового отчёта

✓ титульный лист (наименование ОО, дата, номер отчёта);

✓ вводная часть (дата, время, место, тип инцидента);

✓ подробное описание происшествия (хронология, участники, задействованные системы);

✓ анализ причин (технические, организационные, внешние факторы);

✓ принятые меры (по этапам: оповещение, локализация, устранение, восстановление);

✓ последствия (материальный ущерб, угроза безопасности, простои);

✓ выводы и рекомендации (что улучшить, какие документы актуализировать, обучение персонала);

✓ приложения (фото, логи, протоколы, акты);

✓ подписи ответственных (инженер безопасности, руководитель службы безопасности, директор).

6.3.3. Периодичность

— оперативные отчёты — по факту инцидента;

— промежуточные — в течение суток после инцидента;

— итоговые — в течение 3 рабочих дней после устранения;

— статистические — ежемесячно (до 5-го числа следующего месяца) и ежеквартально (до 10-го числа);

— отчёты для надзорных органов — в сроки, установленные нормативными актами или запросом.

6.4. Хранение и защита данных

6.4.1. Сроки хранения

— карточки инцидентов — не менее 3 лет;

— журнал учёта инцидентов — не менее 5 лет;

— итоговые отчёты и приложения — не менее 5 лет;

— статистические отчёты — не менее 3 лет;

— электронные логи систем КССБ — не менее 6 месяцев (для видеоархива — не менее 30 дней, если не требуется больший срок по локальным актам).

6.4.2. Меры защиты информации

1) Физическая защита:

— бумажные документы хранятся в запираемом шкафу/сейфе;

— доступ в помещение с архивом — по списку уполномоченных;

— учёт выдачи и возврата документов.

2) Электронная защита:

— разграничение прав доступа в информационной системе (роли: оператор, инженер, руководитель, аудитор);

— шифрование конфиденциальных данных (при передаче и хранении);

— резервное копирование (ежедневно, хранение копий вне площадки);

— защита от НСД (двухфакторная аутентификация, журналы аудита действий);

— антивирусная защита и межсетевые экраны.

3) Конфиденциальность:

— запрет на разглашение данных третьим лицам без согласия руководства;

— маркировка документов («Для служебного пользования», «Конфиденциально»);

— подписание обязательств о неразглашении сотрудниками, работающими с данными.

4) Целостность и доступность:

— контроль неизменности записей (хэширование, цифровые подписи);

— восстановление данных из резервных копий в случае сбоев;

— регламентное тестирование систем хранения.

6.4.3. Уничтожение данных:

— по истечении сроков хранения — в порядке, установленном локальным регламентом (с составлением акта уничтожения);

— для электронных данных — с использованием сертифицированных средств стирания;

— для бумажных — путём сжигания или измельчения в шредере**.**

7.1. Перечень экстренных служб, контакты, зоны ответственности

Служба	Контакты	Зона ответственности
Единая дежурно-диспетчерская служба (ЕДДС)	112, 263-34-44, 263-42-10 (факс), 063 (городской бесплатный телефон	Координация действий всех экстренных служб, приём и обработка вызовов, передача информации в соответствующие диспетчерские службы. (**edds.gov74.ru)**

	горячей линии)	
Пожарная служба	101	Тушение пожаров, ликвидация возгораний, спасение людей при пожарах.
Полиция	102	Обеспечение общественного порядка, расследование преступлений, реагирование на чрезвычайные ситуации, связанные с правонарушениями.
Скорая медицинская помощь	103	Оказание экстренной медицинской помощи при угрозах жизни или здоровью.
Аварийная газовая служба	104	Ликвидация утечек газа, аварий на газовых сетях.
Поисково-спасательная служба Челябинской области	735-09-11, 735-01-12, 720-20-99	Проведение поисково-спасательных работ при ЧС.
Главное управление МЧС по Челябинской области	263-41-41	Координация действий при ЧС, связанных с природными и техногенными рисками, организация ликвидации последствий.
УМВД России по г. Челябинску	265-02-00	Обеспечение общественной безопасности, расследование преступлений, координация действий при ЧС на территории города.
Дежурная часть ГИБДД г. Челябинска	256-30-02	Регулирование дорожного движения, реагирование на ДТП, обеспечение безопасности на дорогах при ЧС.

7.2. Порядок оповещения и передачи информации

При возникновении ЧС необходимо немедленно вызвать экстренные службы по номеру 112. Оператор системы-112:

— зарегистрирует вызов и автоматически определит местоположение заявителя;

— заполнит унифицированную карточку информационного обмена, включающую данные о происшествии, времени, месте, контактных данных заявителя;

— передаст карточку в диспетчерские службы, компетентные в решении ситуации.

Диспетчер диспетчерской службы после получения карточки:

— вносит отметку о получении вызова;

— организует реагирование в соответствии с правовыми актами своей организации;

— при необходимости уточняет информацию у заявителя;

— фиксирует в карточке сведения о принятых мерах;

— после завершения реагирования ставит отметку о снятии вызова с контроля.

Оповещение населения также осуществляется через муниципальную систему оповещения, которая включает:

— электромеханические сирены и рупорные громкоговорители;

— сети проводного радиовещания;

— сети уличной радиофикации;

— сети кабельного и эфирного телерадиовещания;

— сети подвижной связи;

— интернет. **(cheladmin.gov74.ru)**

7.3. Совместные действия при ЧС (схемы координации)

Координацию деятельности при ЧС в Челябинске осуществляет ЕДДС города. Она является вышестоящим органом для всех дежурно-диспетчерских служб города по вопросам сбора, обработки, анализа и обмена информацией об угрозе и возникновении ЧС.

Методы организации взаимодействия:

— выработка совместных решений руководителями и должностными лицами;

— образование объединённых штабов и временных органов управления;

— взаимный обмен информацией, относящейся к компетенции сторон;

— совместная разработка планов взаимодействия;

— согласование действий при ликвидации ЧС, включая вопросы обеспечения.

Основные этапы совместных действий:

— сбор и анализ информации о ЧС.

— определение состава привлекаемых служб и ресурсов.

— координация действий сил и средств (пожарной охраны, аварийно-спасательных служб, формирований и т. д.).

— непрерывный контроль за развитием ситуации и корректировка плана действий.

— информирование населения и взаимодействие со СМИ при необходимости.

Для улучшения взаимодействия могут заключаться соглашения между органами власти о территориальных зонах ответственности экстренных служб.

7.4. Документальное сопровождение взаимодействия

Ключевые документы:

Унифицированная карточка информационного обмена. Формируется в системе-112, содержит данные о вызове, передаётся диспетчерским службам. В ней фиксируются все этапы реагирования: получение вызова, принятые меры, завершение работ.

Планы действий. Включают планы действий города Челябинска и организаций по предупреждению и ликвидации ЧС. Они содержат детальные процедуры реагирования, схемы эвакуации, распределение ресурсов и другие меры. (**pravo.gov.ru**)

Соглашения об информационном взаимодействии. Заключаются между оператором системы-112, диспетчерскими службами, ЕДДС, центром управления в кризисных ситуациях и другими участниками системы. В них определяются критерии выбора диспетчерской службы, форматы передаваемой информации, сроки её представления и другие параметры.

Отчёты и статистическая отчётность. Ведётся учёт ЧС, произошедших на территории города, проводятся расследования причин аварий и катастроф, вырабатываются меры по устранению их причин.

Контроль за реагированием на происшествие, анализ и ввод в базу данных информации об основных результатах реагирования, уточнение и корректировка действий привлечённых диспетчерских служб, а также информирование об оперативной обстановке возложены на ЕДДС.

8.1. Периодичность проверок (плановые и внеплановые)

Готовность аварийно-спасательных служб и формирований к реагированию на ЧС проверяется в ходе аттестации, а также при проведении плановых и внеплановых проверок. Их осуществляют:

— Управление по обеспечению безопасности жизнедеятельности населения города Челябинска;

— отраслевые (функциональные) органы Администрации города Челябинска;

— организации, создающие указанные службы и формирования.

Плановые проверки проводятся согласно утверждённым графикам и планам. Например, Главное управление МЧС России по Челябинской области ежегодно формирует планы контрольных (надзорных) мероприятий в области пожарной безопасности, гражданской обороны и защиты от ЧС.

Внеплановые проверки могут проводиться при:

— возникновении ЧС или инцидентов, требующих оценки действий служб;

— поступлении жалоб или обращений о нарушениях в работе служб;

— необходимости оперативного контроля после внесения изменений в нормативные акты или методики работы.

8.2. Критерии эффективности (KPI)

К ключевым показателям эффективности (KPI) в сфере реагирования на ЧС можно отнести:

— время реагирования — срок с момента поступления вызова до начала действий экстренных служб. Например, по регламенту ЕДДС Челябинска приём сообщения должен осуществляться в течение 2 минут, анализ его достоверности — ещё 2 минут, а доведение информации до ответственных служб — в течение 10 минут после подтверждения достоверности;

— процент ложных срабатываний — доля необоснованных вызовов от общего числа поступивших сообщений. Снижение этого показателя свидетельствует о повышении качества обработки информации;

— процент успешно ликвидированных ЧС — доля случаев, когда экстренные службы успешно справились с ситуацией в установленные сроки;

— соблюдение нормативов при выполнении операций (например, контроль мер, принятых по обращению, каждые 30 минут до окончания работ);

— уровень удовлетворённости населения — опросы и анализ жалоб могут показать, насколько граждане довольны скоростью и качеством реагирования.

KPI помогают оценить эффективность работы служб, выявить слабые места и скорректировать стратегию действий. (**calltouch.ru)**

8.3. Порядок актуализации методик

Основания для актуализации методик включают:

— изменения в федеральном и региональном законодательстве (например, новые постановления Правительства РФ, приказы МЧС России);

— появление новых технологий и оборудования, требующих обновления процедур работы;

— результаты проверок и аудитов, выявившие недостатки в существующих методиках;

— опыт реагирования на ЧС, показавший необходимость корректировки алгоритмов действий;

— изменения в структуре рисков (появление новых потенциально опасных объектов, изменение климатических условий и т. д.).

Процедура актуализации может включать:

— анализ изменений и их влияния на существующие методики;

— разработка проектов обновлённых документов (положений, регламентов, инструкций);

— согласование проектов с заинтересованными сторонами (например, с территориальными органами МЧС, другими службами);

— утверждение обновлённых методик компетентным органом (например, Администрацией города Челябинска);

— информирование всех участников системы о внесённых изменениях.

Ответственные за актуализацию — органы, регулирующие деятельность служб (например, Управление по обеспечению безопасности жизнедеятельности населения города Челябинска, ЕДДС, профильные отраслевые органы).

8.4. Обучение персонала

Обучение персонала включает повышение квалификации, тренинги и проверку знаний.

Программы обучения могут включать:

— изучение актуальных нормативных актов и регламентов;

— освоение правил работы с оборудованием и информационными системами (например, системой-112);

— изучение алгоритмов реагирования на различные виды ЧС;

— обучение навыкам коммуникации и координации с другими службами;

— изучение основ гражданской обороны, пожарной безопасности, принципов функционирования систем мониторинга и оповещения.

Тренажи и практические занятия проводятся для отработки навыков в условиях, максимально приближенных к реальным. Это могут быть:

— симуляции ЧС с участием нескольких служб;

— тренировки по эвакуации, ликвидации утечек газа, тушению пожаров и т. д.;

— отработка взаимодействия между диспетчерскими службами и экстренными оперативными службами.

Проверка знаний осуществляется через:

— тестирование после завершения обучения;

— экзамены при аттестации;

— регулярные проверки уровня подготовки в рамках внутренних аудитов служб.

Периодичность обучения зависит от должности и специфики работы. Например, руководители и специалисты дежурно-диспетчерских служб (ДДС) обязаны проходить повышение квалификации регулярно — квалификационное удостоверение действует 5 лет.

Обучение может проводиться в очной, дистанционной или смешанной форме в специализированных учебных центрах.

Пример организации обучения: в Челябинске доступны программы повышения квалификации в учебных центрах, например, в «НЦПО» (курс «Руководитель или специалист ЕДДС муниципальных образований и ДДС организаций») или в «Многопрофильном центре «Феникс» (курс «Основы работы диспетчеров по приёму информации ЕДДЦ реагирования на ЧС и пожары»). **(ncpo.ru)**

Для получения актуальной информации о конкретных программах и требованиях рекомендуется обращаться в уполномоченные органы или учебные центры.

9. Приложения

9.1. Шаблоны документов (карточки инцидента, журналы, отчёты)

9.1.1. Карточка инцидента

(формат: электронный/бумажный, заполняется при первичном фиксировании события)

Регистрационный № _____

Дата и время обнаружения: ____ ч ____ мин, ___ . ____ . 20 __ г.

Место происшествия: здание _____ , этаж ___ , помещение ___ (координаты/зона КССБ).

Тип инцидента (выбрать):

- ✓ сбой СКУД;
- ✓ отказ видеонаблюдения;
- ✓ срабатывание ОПС;
- ✓ инцидент ИБ (атака, утечка);
- ✓ НСД/хулиганство;
- ✓ ЧС (пожар, задымление, угроза теракта);
- ✓ ложное срабатывание.

Краткое описание: _____

Предполагаемая причина: _____ (технический сбой, человеческий фактор, внешнее воздействие)

Задействованные системы КССБ (СКУД, видеонаблюдение, ОПС, СИЕМ, САУ): _____

Обнаруживший (Ф. И. О., должность): _____

Ответственный за реагирование (Ф. И. О., должность): _____

Принятые первичные меры: _____

Статус:

- ✓ в работе;

- ✓ устранён;
- ✓ передан в расследование.

Дата и время закрытия: _____ ч _____ мин, _____ . _____ . 20 __ г.

Подписи:

обнаруживший: _____ (подпись) _____ (Ф. И. О.)

ответственный: _____ (подпись) _____ (Ф. И. О.)

проверяющий: _____ (подпись) _____ (Ф. И. О.)

9.1.2. Журнал учета инцидентов

Обобщенный реестр всех зарегистрированных событий, который ведется в бумажном или электронном виде, включает в себя следующие графы в таблице:

№ п/п

Рег. №

Дата и время

Место

Тип инцидента

Краткое описание

Причина

Системы

Обнаруживший

Ответственный

Меры

Статус

Дата устранения

Приложения

9.1.3. Акт расследования инцидента

Официальный документ для фиксации и расследования инцидента.

Форма № АР-01

Утверждено: Директор _____ /_____/

*Дата введения: «_» **_____** **20** г.*

1. Общие сведения

Показатель	Значение
Регистрационный номер акта	
Дата и время составления акта	___ ч. ____ мин., 20__ г.
Место составления	
Вид инцидента	
Система	
Ответственный за систему	
Дата и время возникновения инцидента	___ ч. ____ мин., 20__ г.
Место происшествия	Здание: _____ Этаж: _____ Помещение / зона: _____

2. Описание инцидента

(Кратко и точно опишите, что произошло, кто обнаружил, как прояви лось, какие системы были задействованы, хронология событий)

_____

_____

_____

_____

_____

3. Установленные причины инцидента

— Корневая причина:

_____

— Косвенные причины (если есть):

_____

— Организационные/технические недостатки:

_____

Пример: *Обрыв кабеля питания камеры из-за несвоевременного техобслуживания; отсутствие резервного канала передачи данных.*

5. Принятые первостепенные меры по устранению последствий

Мера	Ответственный	Срок исполнения	Отметка о выполнении

Пример: *Заменить кабель, восстановить видеозапись, провести инструктаж с персоналом.*

6. Мероприятия по недопущению подробных инцидентов

Мероприятие	Ответственный	Срок исполнения	Отметка о выполнении

Пример: *Ввести график ежемесячных проверок кабельных трасс; ус тановить ИБП на ключевые узлы.*

7. Приложения (перечень)

— Фото/видео фиксация места инцидента

— Логи систем (СКУД, СИЕМ, ОПС)

— Протокол опроса свидетелей

— Акт выявленных неисправностей

— Другое: _____

8. Подписи членов комиссии

Ф. И. О.	Должность	Подпись	Дата

Примечание:

— Акт составляется в **двух экземплярах**: один — в архив организации, второй — ответственному за устранение причин.

— Срок хранения — **не менее 5 лет**.

— При необходимости акт направляется в надзорные органы (МЧС, Роскомнадзор, прокуратура).

9.1. 4. Отчёт о проведённом учении / проверке

(Формируется после тренировок по эвакуации, пожару, ИБ и т.д.)

Структура:

— Дата и время учения.

— Вид учения (пожар, угроза взрыва, кибератака).

— Участники (персонал, МЧС, полиция — если участвовали).

— Ход учения (этапы, действия).

— Выявленные недостатки.

— Рекомендации по устранению.

— Подписи ответственных.

Пример названия: Отчёт № 3/2024 «О проведении учения по эвакуации при пожаре 20.05.2025».

9.1. 5. Журнал проверок технических средств КССБ

(Регулярный контроль оборудования)

№	Дата	Объект проверки	Результат	Выявленные неисправности	Принятые меры	Ответственный	Подпись

9.2. Чек-листы для проверок и аудитов

9.2.1. Чек-лист № 1: Плановая проверка систем КССБ (ежемесячно)

Цель: Оценка работоспособности технических средств и готовности персонала.

№	Пункт проверки	Да / Нет / Не применимо	Комментарии
1	Все камеры видеонаблюдения в рабочем состоянии, изображение чёткое		
2	Запись видеоархива сохраняется не менее 30 суток		
3	СКУД: все точки доступа функционируют, нет несанкционированных открытий		
4	ОПС: датчики дыма, тепла, задымления — в норме, тест сработал		
5	Тревожные кнопки: протестированы, сигнал доходит до ПЦН		
6	Система аварийного оповещения (САУ): звуковая и световая сигнализация работают		
7	СИЕМ (SIEM): логи собираются, нет сбоев в агрегации данных		
8	Резервное питание (ИБП): заряд > 80%, тест пройден		
9	Серверная: доступ только у уполномоченных, температура в норме		
10	Журнал учёта инцидентов ведётся, нет задержек в заполнении		
11	Персонал знает алгоритм действий при ЧС (опрос/тест)		
12	Схемы эвакуации вывешены, не загорожены		

Проверяющий: _____ / _____

Дата: «___» _____ 20 ___ г.

9.2.2. Чек-лист № 2: Аудит взаимодействия с внешними службами (ежеквартально)

Цель: Проверка готовности к вызову и взаимодействию с экстренными службами.

№	Пункт проверки	Да / Нет / Не применимо	Комментарии
1	Контакты экстренных служб (112, МЧС, полиция, скорая) вывешены в ПЦН и у дежурного		
2	Телефонная связь с ЕДДС Челябинска (263-34-44) проверена		
3	Унифицированная карточка информационного обмена доступна (в бумажной и электронной форме)		
4	Проведено тестовое оповещение 112 (учебный вызов, без ложного срабатывания)		
5	Сотрудники знают, как передать информацию: что, кому, в каком порядке		
6	Согласованы маршруты подъезда МЧС и скорой помощи к зданию ОО		
7	Есть акт о взаимодействии с МЧС/полицией (если проводились учения)		
8	Данные о системах КССБ (планы, схемы) переданы в ЕДДС (по требованию)		

Проверяющий: _____ / _____

Дата: «___» _____ 20 ___ г.

9.2.3. Чек-лист 3: Проверка готовности к учениям и ЧС (перед началом учебного года)

№	Пункт проверки	Да / Нет / Не применимо	Комментарии
1	Утверждён план действий при ЧС (пожар, угроза взрыва, НСД)		
2	Проведено инструктажи с персоналом по действиям при ЧС		
3	Проведено не менее одного учения (пожар, эвакуация)		
4	Акты учений оформлены, есть выводы и рекомендации		
5	Схемы эвакуации актуальны, соответствуют планировке		
6	Аптечки первой помощи укомплектованы, срок годности не истёк		
7	Огнетушители на местах, пломбы не нарушены, срок проверки не истёк		
8	Сотрудники знают, где находятся аварийные выходы и запасные маршруты		
9	Родителям направлено уведомление о плане безопасности (по необходимости)		
10	Проведена проверка оповещения через САУ и внутреннюю сеть		

Проверяющий: _____ / _____

Дата: «___» _____ 20 ___ г.

9.2.4. Чек-лист № 4: Аудит информационной безопасности (раз в полгода)

№	Пункт проверки	Да / Нет / Не применимо	Комментарии
1	Установлены актуальные версии ПО на серверах и рабочих станциях		
2	Антивирусное ПО обновлено, сканирование регулярное		
3	Учётные записи пользователей: нет неиспользуемых, пароли сложные		
4	Доступ к СИЕМ и журналам — только у администратора		
5	Проведена проверка на уязвимости (сканирование сети)		
6	Есть резервное копирование данных (не менее 2 копий, 1 — вне сети)		
7	Проведён тест восстановления данных из резервной копии		
8	Зафиксированы и проанализированы все инциденты ИБ за период		
9	Сотрудники прошли обучение по фишингу и социальной инженерии		
10	Есть политика ИБ, ознакомлены все сотрудники		

Проверяющий: _____ / _____

Дата: «___» _____ 20 ___ г.

9.2.5. Чек-листы для ответственных лиц при ИБ-инциденте

Пошаговый план действий при обнаружении инцидента ИБ в КССБ образовательной организации

1. Фиксация факта

Цель: документально зафиксировать первичные данные об инциденте.

Действия:

— зафиксировать точную дату и время обнаружения;

— указать источник информации (система защиты, пользователь, мониторинг);

— описать наблюдаемые симптомы (ошибки, поведение системы, сообщения);

— перечислить затронутые ресурсы (серверы, ПК, сети, приложения);

— сохранить скриншоты интерфейсов, сообщений об ошибках.

Чек-лист № 1. Фиксация факта

— дата и время зафиксированы;

— источник информации указан (SIEM, пользователь, сканер и т. д.);

— симптомы описаны (конкретно: что наблюдается);

— затронутые ресурсы перечислены (серверы, ПК, сети и т. п.);

— скриншоты/логи сохранены (при наличии);

— ответственный за фиксацию указан (ФИО, должность).

Значимость: создаёт доказательную базу, позволяет восстановить хронологию.

2. Первичная оценка

Цель: определить масштаб и приоритет инцидента для выбора стратегии реагирования.

Действия:

— оценить масштаб (единичный узел / сегмент сети / вся инфраструктура);

— классифицировать тип инцидента (фишинг, утечка, вредоносное ПО и т. д.);

— определить приоритет (высокий/средний/низкий) по критериям организации;

— оценить потенциальный ущерб (конфиденциальность, целостность, доступность данных);

— принять решение о необходимости изоляции.

Чек-лист № 2. Первичная оценка

— масштаб оценён (единичный/сегмент/вся сеть);

— тип инцидента предварительно определён;

— приоритет установлен (высокий/средний/низкий);

— потенциальный ущерб оценён (ПДн, финансы, репутация и т. д.);

— решение об изоляции принято (да/нет);

— ответственные за реагирование назначены.

Значимость: определяет скорость и объём необходимых мер.

3. Изоляция

Цель: предотвратить распространение угрозы и минимизировать ущерб.

Действия:

— отключить затронутый узел от сети (физически или программно);

— заблокировать подозрительные учётные записи;

— изменить пароли скомпрометированных аккаунтов;

— настроить правила блокировки на межсетевом экране (IP, порты, протоколы);

— изолировать сегменты сети при необходимости;

— ограничить доступ к затронутым ресурсам.

Чек-лист № 3. Изоляция

— затронутый узел отключён от сети;

— подозрительные учётные записи заблокированы;

— пароли изменены (если требуется);

— правила МЭ настроены (блокировка IP/портов);

— сегменты сети изолированы (если нужно);

— доступ к ресурсам ограничен;

— действия документированы (что и когда заблокировано).

Значимость: останавливает распространение угрозы, сохраняет доказательства.

4. Уведомление

Цель: своевременно информировать ответственных лиц и внешние органы.

Действия:

— уведомить руководство организации (директор, зам по ИТ);

— сообщить ИТ-отделу и службе безопасности;

— при необходимости — направить уведомление в ГосСОПКА;

— информировать затронутых пользователей (если требуется);

— зафиксировать факт уведомления (кому, когда, каким способом).

Чек-лист № 4. Уведомление

— руководство уведомлено (ФИО, время, способ);

— ИТ-отдел и СБ проинформированы;

— ГосСОПКА уведомлена (если требуется, № обращения);

— пользователи проинформированы (если нужно, способ);

— факт уведомления документирован (дата, время, получатели).

Значимость: обеспечивает координацию действий, соответствие требованиям регуляторов.

5. Сбор доказательств

Цель: сохранить данные для расследования и возможного судебного разбирательства.

Действия:

— скопировать журналы событий (ОС, приложений, сетевого оборудования);

— сделать скриншоты интерфейсов, сообщений;

— создать дампы памяти затронутых систем;

— сохранить образцы вредоносного ПО (в изолированной среде);

— зафиксировать конфигурацию систем на момент инцидента;

— обеспечить целостность собранных данных (хеширование, защита от изменений).

Чек-лист № 5. Сбор доказательств

— журналы событий скопированы (какие, откуда);

— скриншоты сделаны (что зафиксировано);

— дампы памяти созданы (если требуется);

— образцы вредоносного ПО сохранены (в безопасной среде);

— конфигурация систем зафиксирована;

— целостность данных обеспечена (хеши, защита от изменения);

— место хранения доказательств определено.

Значимость: формирует доказательную базу для расследования и юридических действий.

6. Расследование

Цель: установить причины, хронологию и последствия инцидента.

Действия:

— проанализировать собранные доказательства (логи, дампы, скриншоты);

— восстановить хронологию событий (, и т. д.);

— выявить уязвимости, использованные злоумышленником;

— определить источник атаки (IP, домен, вектор);

— оценить фактический ущерб (данные, системы, время простоя);

— установить причастных лиц (внутренние/внешние).

Чек-лист № 6. Расследование

— доказательства проанализированы;

— хронология событий восстановлена;

— уязвимости выявлены (какие, где);

— источник атаки определён (IP, вектор и т. п.);

— ущерб оценён (данные, время, финансы);

— причастные лица установлены (если возможно);

— предварительные выводы сформулированы.

Значимость: позволяет понять механизм инцидента и предотвратить повторение.

7. Устранение

Цель: нейтрализовать угрозу и восстановить штатную работу систем.

Действия:

— удалить вредоносное ПО, устранить уязвимости;

— восстановить затронутые данные из резервных копий;

— вернуть системы в рабочее состояние;

— проверить отсутствие скрытых угроз (повторное сканирование);

— обновить конфигурации и политики безопасности;

— протестировать работоспособность сервисов.

Чек-лист № 7. Устранение

— угроза нейтрализована (что удалено/исправлено);

— данные восстановлены (из каких копий);

— системы возвращены в работу;

— скрытые угрозы не обнаружены (результаты сканирования);

— конфигурации обновлены (какие изменения внесены);

— работоспособность проверена (тесты пройдены);

— время восстановления зафиксировано.

Значимость: восстанавливает функциональность инфраструктуры, закрывает уязвимости.

8. Отчётность

Цель: документировать инцидент и принятые меры для анализа и отчётности.

Действия:

— заполнить журнал регистрации инцидентов;

— оформить первичный отчёт (факт, меры, ущерб);

— подготовить итоговый отчёт по расследованию (хронология, причины, рекомендации);

— передать отчёты руководству и регуляторам (если требуется);

— архивировать материалы расследования.

Чек-лист № 8. Отчётность

— запись в журнале инцидентов сделана (номер, дата, описание);

— первичный отчёт оформлен (что зафиксировано);

— итоговый отчёт подготовлен (хронология, выводы, рекомендации);

— отчёты переданы (кому, когда);

— материалы архивированы (место хранения, срок);

— статус инцидента обновлён (закрыт/в работе).

Значимость: обеспечивает прозрачность, соответствие требованиям, базу знаний.

9. Профилактика

Цель: минимизировать риск повторения аналогичных инцидентов.

Действия:

— скорректировать регламенты и процедуры ИБ;

— провести дополнительное обучение персонала;

— обновить ПО и конфигурации систем;

— внедрить дополнительные меры защиты (если требуется);

— запланировать повторные аудиты и тестирования;

— распространить уроки инцидента среди сотрудников.

Чек-лист № 9. Профилактика

— регламенты скорректированы (какие изменения);

— обучение проведено (кто, когда, тема);

— ПО обновлено (версии, патчи);

— новые меры защиты внедрены (какие);

— аудиты/тесты запланированы (сроки, объём);

— уроки инцидента распространены (как, среди кого);

— план профилактики утверждён (кем, когда).

Значимость: повышает устойчивость системы ИБ, снижает вероятность повторных угроз.