МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ 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

Совершенствование системы защиты информации в образовательной организации СПО

Магистерская диссертация
по направлению 44.04.04 Профессиональное обучение
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»

Выполнил:
студент группы ЗФ-309/210-2-1,
Чупахина Ирина Сергеевна
Научный руководитель:
д.т.н., профессор
кафедры АТ, ИТ и МОТД
Дмитриев Михаил Сергеевич

Проверка на объём заимствований:
65,31 авторского текста
Работа рекомендована к защите
«01» февраля 2019 г.
Зав. кафедрой АТ, ИТ и МОТД
_____ В. В. Руднев

Челябинск, 2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
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

Направление подготовки: 44.04.04. -
Профессиональное обучение (по отраслям)
Направленность (профиль): Управление информационной безопасностью в профессиональном образовании

ЗАДАНИЕ
на магистерскую диссертацию

Магистранту группы ЗФ-309/210-2-1 заочного отделения Чупахиной Ирине Сергеевне, обучающейся по программе магистратуры «Управление информационной безопасностью в профессиональном образовании».

Научный руководитель выпускной квалификационной работы: Дмитриев М.С., д.т.н., профессор кафедры АТ, ИТ и МОТД.

1.Тема квалификационной работы: «Совершенствование системы защиты информации в организации СПО», утверждена приказом Южно-уральского государственного гуманитарно-педагогического университета № 580-сз от «26» апреля 2017 г.

2. Материалы для выполнения магистерской диссертации:

2.1. Учебная, научно-техническая, педагогическая, методическая литература по теме магистерской диссертации: отчет по преддипломной практике в ГБПОУ «ЮУГК», нормативная и законодательная документация, специальная литература, периодические издания, Интернет.

3. Основные части магистерской диссертации (перечень подлежащих разработке вопросов) и сроки их выполнения представлены в нижеприведенной таблице:

Календарный план работы

	Перечень вопросов, подлежащих разработке в диссертации	Сроки
1	ВВЕДЕНИЕ Оговаривается значение и актуальность темы работы, объект и предмет исследования,	15.05.2017

	проблема, цель и задачи работы, пути их решения. Указываются методы исследования.	
2	Глава 1. Теоретические аспекты обеспечения информационной безопасности в организациях профессионального образования Выводы по главе 1	16.10.2017
3	Глава 2. Анализ информационной безопасности в организации профессионального образования Выводы по главе 2	23.04.2018
4	Глава 3. Совершенствование систем информационной безопасности в организации профессионального образования Выводы по главе 3	29.12.2018
5	ЗАКЛЮЧЕНИЕ (объем в пределах 3 стр.) Содержит кратко и четко сформулированные выводы, и рекомендации.	29.12.2018
6	СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ (сначала располагаются нормативно – законода-тельные акты, остальные источники в алфавитном порядке). Законы и нормативные акты, справочно-статистические материалы, учебники, сборники брошюры, статьи из периодической печати, иностранная литература.	29.12.2018
7	ПРЕЗЕНТАЦИЯ (НАГЛЯДНЫЕ МАТЕРИАЛЫ) предоставляется в виде слайдов рекомендаций Microsoft PowerPoint, 10-12 слайдов, раскрывающих содержание магистерской диссертации, либо схемы, таблицы, графики, диаграммы в виде раздаточного материала	28.01.2019
	ПРЕДВАРИТЕЛЬНАЯ ЗАЩИТА	28.01.2019
	СДАЧА МАГИСТЕРСКОЙ ДИССЕРТАЦИИНА КАФЕДРУ	18.02.2019

Дата выдачи задания «27»__апреля__ 2017 года

Заведующий кафедрой АТ, ИТ и МОТД
Наименование кафедры

_____
Ф.И.О., ученое звание и степень Подпись заведующего кафедрой

Задание выдал: _____
Ф.И.О., ученое звание и степень Подпись научного руководителя

Задание принял_____
Ф.И.О магистранта Подпись магистранта

Содержание

ВВЕДЕНИЕ

Актуальность темы. Совершенствование системы обеспечения информационной безопасности на предприятиях, фирмах и организациях, в частности в образовательных учреждениях очень важно в современном мире.

Под системой обеспечения информационной безопасности (ИБ) понимается совокупность документированных управленческих решений, направленных на защиту информационных ресурсов организации.

Отсутствие современной, правильно выстроенной системы обеспечения безопасности в организации, может привести к потере важной информации, что приводит к большим издержкам материального характера, потере персональных данных сотрудников организации, ущерб для имиджа, поэтому необходимо уделять пристальное внимание вопросам информационной безопасности.

Информационная безопасность (на уровне предприятий и организаций) - это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести недопустимый ущерб субъектам информационных отношений.

В отечественной и зарубежной литературе в настоящее время немалое внимание уделяется проблемам информационной безопасности.

Более подробно во второй половине XX века проблему исследования информационной политики, развития информационного пространства в Российской Федерации были рассмотрены в работах: М.С. Вершинина, К.В. Ветрова, С.Э. Зуева, В.Д. Попова, А.И. Ракитова.

Особый вклад в исследование информационной безопасности в различных сферах общества, культуры, науки и техники, внесли такие ученые и исследователи, как А.Б. Агапов, А.С. Алексеев, И.Л. Бачило, А.В. Возженников, Ю.М. Горский, Г.Н. Горшенков, И.С. Даниленко, Н.В. Данилов, С.А. Дятлов,

Г.Г. Феоктистов, А.М. Яновский и другие. В работах этих ученых сформулированы концептуальные положения о сущности и содержании категорий информационной безопасности, исследованы их взаимосвязи, обоснованы приемы и способы исследования информационной безопасности и различных составляющих системного подхода.

Важное значение с точки зрения объекта и предмета настоящего исследования имеют также работы А.В. Кульбы, А.С. Рябцева, К.В. Станиславчика, А.Б. Табакова.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения информации имеет особое значение. К таким информационным системам можно отнести, например, банковские или юридические системы безопасного документооборота и другие информационные системы, для которых обеспечение защиты информации является жизненно важным.

В настоящее время, несмотря на большое количество работ по проблематике, следует отметить, что ее теоретическая изученность явно недостаточна, практические методики по формированию оптимального механизма информационной безопасности в образовательных организациях не соответствуют условиям реального времени. В работах отечественных и западных авторов превалирует односторонний подход в исследовании проблем информационной безопасности, рассматривается какая-то одна сторона из всего механизма информационной безопасности в организациях вообще.

Для того чтобы отразить подход организации к защите своих информационных активов необходимо разработать политику информационной безопасности, каждая организация должна осознать необходимость поддержания соответствующего режима безопасности и выделения на эти цели значительных ресурсов.

Политика информационной безопасности - свод документов, в которых рассматриваются вопросы организации, стратегии, методов и процедур в

отношении конфиденциальности, целостности и доступности информационных ресурсов организации. Политика безопасности строится на основе анализа рисков - процесса определения угроз безопасности системы и отдельным ее компонентам, определение их характеристик и потенциального ущерба.

Конечная цель разработки политики информационной безопасности - обеспечить целостность, доступность и конфиденциальность для каждого информационного ресурса.

Таким образом, потребность в создании оптимальной системы информационной безопасности, а также проработка вопроса использования более совершенных методов обеспечения информационной безопасности образовательных организаций определили объект, предмет, цель и основные задачи исследования.

Цель исследования заключается в анализе методов и инструментов совершенствования системы информационной безопасности для обеспечения и повышения информационной безопасности организаций профессионального образования

Объектом исследования является система информационной безопасности образовательных организациях

Предмет исследования: Внедрение системы мониторинга корпоративной сети ГБПОУ «Южно-Уральского государственного колледжа».

Реализация поставленной цели в магистерской диссертации потребовала постановки и последовательного решения следующих взаимосвязанных **задач**:

1. Раскрыть сущность и содержание системы информационной безопасности в организациях профессионального образования; дать характеристику угроз информационной безопасности;

2. Изучить объект защиты - ГБПОУ «Южно-Уральский государственный колледж», его структуру, информационные ресурсы и информационные потоки колледжа; проанализировать систему обеспечения информационной

безопасности в ГБПОУ ЮУрГТК; выявить уязвимости в системе защиты информации;

3. Разработать концепцию информационной безопасности колледжа ГБПОУ «Южно-Уральский государственный колледж», внедрить средства для повышения информационной безопасности и оценить их эффективность.;

4. Разработать рекомендации по применению средств и методов совершенствования системы информационной безопасности ГБПОУ «Южно-Уральский государственный колледж»;

Научная новизна исследования состоит в комплексном решении актуальной задачи, состоящей в совершенствовании системы обеспечения информационной безопасности организаций профессионального образования, позволяющей повысить уровень устойчивости информационной безопасности колледжа.

Методологическую основу исследования составили законодательные и нормативно-правовые документы РФ, разработки в области обеспечения информационной безопасности, методы и способы построения процессов управления информационной безопасностью в целях повышения ИБ в организациях, системный анализ.

Теоретическую и информационную базу исследования составляют основные положения по информационной безопасности, системный подход к исследуемому объекту и предмету, в качестве информационных источников использованы аналитические и статистические материалы по информационной безопасности, материалы научных конференций, средств массовой информации, отражающие аспекты информационной безопасности.

Научно - практическая ценность работы заключается в том, что основные положения, выводы и рекомендации диссертационного исследования нацелены на совершенствование системы обеспечения информационной безопасности организаций профессионального образования. Проведенные исследования и полученные результаты составляют теоретическую основу моделирования, совершенствования системы обеспечения информационной

безопасности образовательных организаций. Рассмотренные методы направлены на решение задачи по повышению эффективности информационной безопасности образовательных организаций.

Практическая значимость заключается в разработке концепции информационной безопасности организации среднего профессионального образования и разработке рекомендаций по усилению защиты информации в ГБПОУ «Южно-Уральский государственный колледж».

Структура магистерской диссертации: введение, три главы, выводы по главам, заключение, библиографический список.

Глава 1. ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

1.1. Сущность и содержание системы информационной безопасности в организациях среднего профессионального образования

Достижения научно-технического прогресса позволяют автоматизировать любой процесс в любой сфере деятельности человека. Система образования не исключение. С появлением автоматизированных систем обработки данных изменился формат хранения и использования информации.

В связи с этим возникла проблема защиты информации и обеспечения безопасности ее использования и хранения.

Прежде чем рассмотреть сущность информационной безопасности в образовании, следует дать общее определение понятию информационной безопасности.

Информационной безопасностью называется защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. [1]

В понятие информационной безопасности образовательной организации входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы. Вторым аспектом понятия станет защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

В составе массивов охраняемой законом информации, находящейся в распоряжении образовательной организации, можно выделить три группы:

- персональные сведения, касающиеся обучающихся и преподавателей, оцифрованные архивы;
- ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;
- структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

Все эти сведения не только могут стать объектом хищения. Намеренное проникновение в них может нарушить сохранность оцифрованных книг, уничтожить хранилища знаний, внести изменения в код программ, используемых для обучения.

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

– доступности в любое время для любого авторизированного пользователя;

– защиты от любой утраты или внесения несанкционированных изменений;

– конфиденциальности, недоступности для третьих лиц.

На основании этого система обеспечения информационной безопасности организации рассматривается как целый комплекс принятых управленческих решений, направленных на выявление и предотвращение внешних и внутренних угроз. Эффективность принятых мер основывается на определении таких факторов, как степень и характер угрозы, аналитическая оценка кризисной ситуации и рассматривание других неблагоприятных моментов, представляющих опасность для развития организации и достижения поставленных целей. Обеспечение информационной безопасности организации базируется на принятии таких мер, как:

1. Анализ потенциальных и реальных ситуаций, представляющих угрозу безопасности информации образовательной организации;

2. Оценка характера угроз безопасности информации;

3. Принятие и комплексное распределение мер для определения угрозы;

4. Реализация принятых мер по предотвращению угрозы.

Основная цель обеспечения комплексной системы безопасности информации для защиты образовательной организации, это:

– создать благоприятные условия для нормального функционирования в условиях нестабильной среды;

– обеспечить защиту собственной безопасности;

– возможность на законную защиту собственных интересов от противоправных действий конкурентов;

– обеспечить сотруднику и студенту сохранностью жизни и здоровья.

– предотвращать возможность материального и финансового хищения, искажения, разглашения и утечки конфиденциальной информации, растраты, производственные нарушения, уничтожение имущества и обеспечить нормальную производственную деятельность.

Обеспечение безопасности информации любой организации основывается на следующих критериях:

– соблюдение конфиденциальности и защита интеллектуальной собственности;

– предоставление физической охраны для персонала предприятия;

– защита и сохранность имущественных ценностей.

Организация обеспечения безопасности образовательной организации основывается на тех же принципах защиты и предполагает постоянную модернизацию защитных функций, поскольку эта сфера постоянно развивается и совершенствуется. Казалось бы, еще недавно созданные новые защитные системы со временем становятся уязвимыми и недействительными, вероятность их взлома с каждым годом возрастает.

В связи с этим система безопасности образовательного учреждения должна совершенствоваться постоянно. Существует ряд принципов, которых необходимо придерживаться при разработке и совершенствовании систем информационной безопасности:

1. обеспечение безопасности новых типов информационных ресурсов;
2. организация доверенного взаимодействия сторон (взаимной идентификации / аутентификации) в информационном пространстве;
3. защита от автоматических средств нападения;
4. интеграция в качестве обязательного элемента защиты информации в процессе автоматизации ее обработки.

1.2. Характеристика угроз информационной безопасности в учреждениях среднего специального образования

Угроза безопасности информации – потенциальная возможность нарушения основных качественных характеристик (свойств) информации при её обработке техническими средствами: конфиденциальности, целостности, доступности [12].

Под угрозами конфиденциальной информации принято понимать потенциальные или реально возможные действия по отношению к информационным ресурсам, приводящие к неправомерному овладению охраняемыми сведениями.

Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. [4]

Такими действиями являются:

- ознакомление с конфиденциальной информацией различными путями и способами без нарушения её целостности;
- модификация информации в криминальных целях как частичное или значительное изменение состава и содержания сведений;
- разрушение (уничтожение) информации как акт вандализма в целях прямого нанесения материального ущерба.

В конечном итоге противоправные действия с информацией приводят к нарушению её конфиденциальности, полноты, достоверности и доступности, что в свою очередь приводит к нарушению как режима управления, так и его качества в условиях ложной или неполной информации.

Каждая угроза влечёт за собой определённый ущерб – моральный или материальный, а защита и противодействие угрозе призвано снизить его величину, в идеале – полностью, реально – значительно или хотя бы частично. Но и это удаётся далеко не всегда [12].

С учётом этого угрозы могут быть классифицированы по следующим кластерам:

1. по величине принесённого ущерба:
   - предельный, после которого образовательная организация может стать банкротом
   - значительный, но не приводящий к банкротству
   - незначительный, который образовательная организация может компенсировать и др.
2. по вероятности возникновения:
   - весьма вероятная угроза
   - вероятная угроза
   - маловероятная угроза

3. по причинам появления:
   - стихийные бедствия
   - преднамеренные действия
4. по характеру нанесённого ущерба:
   - материальный
   - моральный
5. по характеру воздействия:
   - активные
   - пассивные
6. по отношению к объекту:
   - внутренние
   - внешние

Источниками внешних угроз являются:

1. недобросовестные конкуренты
2. преступные группировки и формирования
3. отдельные лица и организации административно-управленческого аппарата

Источниками внутренних угроз могут быть:

1. администрация организации
2. персонал
3. технические средства обеспечения производственной и трудовой деятельности [12]

С точки зрения проникновения в периметр информационной безопасности и для совершения хищения информации или создания нарушения в работе систем необходим несанкционированный доступ.

Способы несанкционированного доступа

Можно выделить несколько видов несанкционированного доступа:

1. Человеческий. Информация может быть похищена путем копирования на временные носители, переправлена по электронной

почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

2. Программный. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.
3. Аппаратный. Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

Каждая угроза должна быть учтена и оценена специалистами. Поэтому важно определить критерии оценки опасности возникновения угрозы и вероятности поломки или обхода защиты информации. Показатели подсчитываются с помощью применения ранжирования. Среди всех критериев выделяют три основных:

1. Доступность – это критерий, который учитывает, насколько удобно источнику угроз использовать определенный вид уязвимости, чтобы нарушить информационную безопасность. В показатель входят технические данные носителя информации (вроде габаритов аппаратуры, ее сложности и стоимости, а также возможности использования для взлома информационных систем неспециализированных систем и устройств).
2. Фатальность – характеристика, которая оценивает глубину влияния уязвимости на возможности программистов справиться с последствиями созданной угрозы для информационных систем. Если оценивать только объективные уязвимости, то определяется их информативность – способность передать в другое место полезный сигнал с конфиденциальными данными без его деформации.
3. Количество – характеристика подсчета деталей системы хранения и реализации информации, которым присущ любой вид уязвимости в системе.

Если описывать классификацию угроз, которые обходят защиту информационной безопасности, то можно выделить несколько классов:

1. Ранг преднамеренности совершения вмешательства в информационную систему защиты:
   - угроза, которую вызывает небрежность персонала в информационном измерении;
   - угроза, инициатором которой являются мошенники, и делают они это с целью личной выгоды.
2. Характеристики появления:
   - угроза информационной безопасности, которая провоцируется руками человека и является искусственной;
   - природные угрожающие факторы, не подконтрольные информационным системам защиты и вызывающиеся стихийными бедствиями.
3. Классификация непосредственной причины угрозы. Виновником может быть:
   - человек, который разглашает конфиденциальную информацию, орудуя с помощью подкупа сотрудников компании;
   - природный фактор, приходящий в виде катастрофы или локального бедствия;
   - программное обеспечение с применением специализированных аппаратов или внедрение вредоносного кода в техсредства, что нарушает функционирование системы;
   - случайное удаление данных, санкционированные программно-аппаратные фонды, отказ в работе операционной системы.

Существует еще одна классификация источников угроз информационной безопасности. Она основана на других параметрах и также учитывается во время анализа неисправности системы или ее взлома. Во внимание берется следующее:

Состояние источника угрозы:

- в самой системе, что приводит к ошибкам в работе и сбоям
- вне системы, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных;
- мошенничество. Случаи, когда информация захватывается во время прохождения по путям связи, побочный захват с акустических или электромагнитных излучений устройств.

Степень влияния:

- активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность
- та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.

Возможность доступа сотрудников к системе программ или ресурсов:

- вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного);
- вред наносится после согласия доступа к ресурсам системы.

Выводы по главе 1.

На основании рассмотренного в данной главе теоретического материала, можно сделать следующие выводы:

1. Существует множество угроз для информационного пространства образовательного учреждения. Их классификация обширна, но, по сути, все угрозы можно поделить на две большие группы: внутренние и внешние. Обе этих разновидности в равной степени представляют большую опасность для данных информационного пространства образовательного учреждения.
2. Чем больше процессов подвергается автоматизации и большее количество данных переносится с бумажных носителей в информационную среду образовательного учреждения, тем насущнее становится необходимость совершенствования средств защиты информации и их широкого внедрения в практику организаций СПО.
3. Среда защиты информации должна включать в себя комплекс средств контроля потоков информации, доступа к информационной среде образовательного учреждения, мониторинга и защиты локальных сетей, а также информации, поступающей из глобальных сетей.

На основании изложенных теоретический изысканий можно произвести анализ обеспечения информационной безопасности в организации СПО, выявить ее слабые стороны и уязвимости.

ГЛАВА 2. АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

2.1. Общие сведения об организации профессионального образования

Южно-Уральский государственный колледж расположен по адресу: г. Челябинск, ул. Курчатова, 7.

Учредителем колледжа является Министерство образования и науки Челябинской области.

ГБПОУ «Южно-Уральский государственный колледж» является старейшим в Уральском регионе государственным средним профессиональным образовательным учреждением повышенного типа. Главная цель и направление деятельности ГБПОУ «Южно-Уральский государственный колледж» – повышение качества знаний и уровня профессиональных компетенций выпускников колледжа за счет разработки, создания и внедрения инновационных образовательных технологий, основанных на E-Learning, электронных учебно-методических комплексах, компетентностном подходе. Данные технологии и формы обучения позволили реально повысить качество профессиональной подготовки, прежде всего практического обучения, и сделали выпускников колледжа востребованными на рынке труда.

На протяжении ряда лет Южно-Уральский государственный колледж (бывший Челябинский колледж информационно-промышленных технологий и художественных промыслов, бывший Челябинский экономический 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 колледжу активно решать проблемы доступности, эффективности и качества профессиональной подготовки современных специалистов для отраслей предприятий России.

Колледж сегодня специализируется на подготовке бухгалтеров, финансистов, коммерсантов, менеджеров, маркетологов, юристов, техников автоматизированных систем обработки информации и управления, дизайнеров.

Педагоги колледжа имеют опыт практической работы по соответствующей специальности и глубокую теоретическую подготовку, необходимую для успешной реализации профессиональных образовательных программ. Среди них — кандидаты наук, заслуженные работники образования РФ, 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» (создан в 1953 г.) и ГБОУ СПО (ССУЗ) «Челябинский колледж промышленной автоматики» (создан в 1953 г.), которые в дальнейшем определили три образовательных комплекса (по территориальному признаку и направлениям подготовки):

- Информационных технологий и экономики (ул. Курчатова, д.7);
- Промышленной автоматики (ул. Доватора, д.38);
- Промышленного дизайна и торговли (ул. Блюхера, ул.1А).

Непосредственное управление деятельностью колледжа осуществляет директор.

Руководство и педагогический состав

Управление Колледжем осуществляется в соответствие с законодательством Российской Федерации и Уставом учебного заведения. Общее руководство Колледжа осуществляет выборный представительный орган – Совет колледжа, в состав которого входят представители всех категорий работников, студенты. Председателем Совета по должности является директор колледжа. Решение Совета колледжа проводится в жизнь приказом директора. Срок полномочия Совета колледжа составляет 5 лет.

В целях совершенствования качества обучения и воспитания студентов, повышения педагогического мастерства преподавателей в Колледже создан и

действует учебно-методический Совет, объединяющий педагогических работников. Председателем Совета является заместитель директора по учебной работе. Совет организует работу по методическому обеспечению учебного процесса, планирует и направляет разработку и издание учебно-методических пособий в бумажном и электронном вариантах, занимается внедрением новейших информационных образовательных технологий.

Воспитательная работа с участием молодежи осуществляется педагогическим коллективом в ходе всего образовательного процесса, а также через студенческое самоуправление, организованное в колледже и в общежитии. Высшим органом студенческого самоуправления является Совет самоуправления колледжа, который координирует работу Советов учебных групп и общежития [13].

Непосредственное управление деятельностью колледжа осуществляет директор. Директор назначается Учредителем.

Лапин Владимир Геннадьевич - директор колледжа.

Калиновская Татьяна Сергеевна - заместитель директора по учебной работе.

Милюков Иван Васильевич - заместитель директора по производственному обучению.

Торопов Андрей Алексеевич - заместитель директора по учебно-практической работе.

Насеретдинова Эльвира Борисовна - заместитель директора по инновационно-методической работе.

Фадеев Виталий Олегович - заместитель директора по административно-хозяйственной работе.

Абзалова Алла Геннадьевна - главный бухгалтер.

Организационная структура колледжа представлена на рисунке 1.

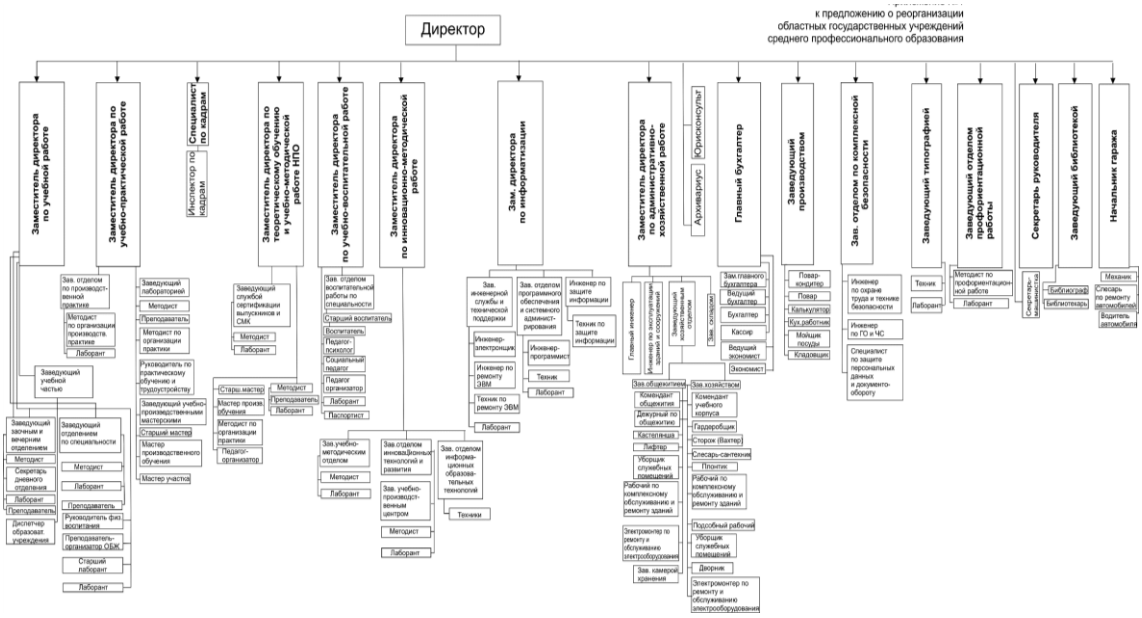


Рис. 1 – Структура колледжа ГБПОУ «Южно-Уральский государственный колледж

2.2. Политика безопасности организации профессионального образования.

Пользование информационными ресурсами ГБПОУ «Южно-Уральский государственный колледж» регламентируется в соответствии с Федеральным законом «Об образовании в Российской Федерации» от 29 декабря 2012 г. № 273-ФЗ.

Доступ педагогических работников и обучающихся к информационным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной Уставом колледжа.

Исследуемое предприятие содержит следующие информационные ресурсы:

информация, относящаяся к коммерческой тайне:

– заработная плата,

– договоры с поставщиками и арендаторами.

защищаемая информация:

– личные дела работников и обучающихся;

– трудовые договора;

– личные карты работников;

– содержание регистров бухгалтерского учета и внутренней бухгалтерской отчетности;

– прочие разработки и документы для внутреннего пользования.

открытая информация:

– буклеты,

– информация на web-сайте **www.ecol.edu.ru**,

– учредительный документ,

– устав,

– перечень образовательных программ и т. д.

Доступ к информационно-телекоммуникационным сетям: доступ педагогических работников к информационно-телекоммуникационной сети Интернет в колледже осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет. Для доступа к информационно-телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные данные (логин и пароль / учётная запись). Предоставление доступа осуществляется системным администратором колледжа.

Рассмотрим политику безопасности данного колледжа. Установлен порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности.

Система обеспечения информационной безопасности в колледже осуществляется комплексно и включает в себя меры следующих уровней:

1 уровень: Нормативно–правовой, включающий законы, постановления правительства и указы президента, нормативные акты и стандарты, которыми регламентируются правила использования и обработки информации

ограниченного доступа, а также вводятся меры ответственности за нарушения этих правил.

Основными законодательными актами, регулирующими вопросы информационной безопасности колледжа, являются:

– Гражданский кодекс РФ ст.139;

– Уголовный кодекс гл.28 ст.272, 273, 274, 138, 183;

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» в действующей редакции.

– Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в действующей редакции.

– Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2 уровень: Организационно-административный.

Организационные меры являются решающим звеном формирования и реализации комплексной защите информации. Эти меры играют существенную роль в создании надежного механизма защиты информации, т.к. возможности несанкционированного использования конфиденциальных сведений в значительной мере обуславливаются не техническими аспектами, а злоумышленными действиями, небрежностью пользователей или персонала защиты.

Организационные меры защиты информации в колледже реализованы следующим образом:

– организован контроль, соблюдение временного режима труда и пребывания сотрудников колледжа на территории организации;

– организована работа с документами и документированной информацией, т.е. ведется учет, исполнение, возврат, хранение носителей конфиденциальной информации;

– администрирование сети и разграничением прав пользователей. Политика безопасности домена предписывает пользователям регулярно изменять свои пароли, контролирует не повторяемость и непохожесть паролей.

В качестве недостатков данного уровня защиты можно указать следующие факты.

В колледже отсутствует обучение пользователей ИС, периодические инструктажи, наказания/поощрения пользователей, что ведет к небрежности сотрудников, выраженная в недостаточном знании правил защиты конфиденциальной информации, непониманием необходимости тщательного их выполнения и студентов, заключающаяся в частоте блокирование системы из-за неправильности введенных данных.

А также на административном уровне политика информационной безопасности пока не утверждена.

3 уровень: Программно-аппаратный.

Программно-технические меры защиты информации - это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности информации.

В колледже осуществляется управление доступом путем деления информации по соответствующим должностям и полномочиям доступа к ней, т.е. спецификация и контроль действий пользователей над информационными ресурсами колледжа.

Программно-аппаратные средства защиты информации:

1. SHDSL-модем с возможностью работать в режиме маршрутизатора для закрытия сети от проникновения извне.

SHDSL модем ZyXEL предназначен для создания корпоративной сети, в основе которой лежит скоростное двунаправленное соединение по медным проводам. Используется для объединения двух офисов по одной или по двум

медным парам в режиме «точка-точка» с организацией симметричного скоростного полнодуплексного соединения. Модем имеет возможность работать в режиме моста или маршрутизатора. Встроена система обнаружения и предотвращения вторжений (Intrusion Detection System - IDS).

2. Антивирусная система Kaspersky Anti-Virusдля защиты от компьютерных вирусов. Производится нерегулярное обновление баз и сканирование рабочих станций.

2.3. Корпоративная сеть образовательной организации СПО: структура, сетевое оборудование, технические характеристики, протоколы, защищенность.

Корпоративная сеть имеет огромное значение для активно развивающейся информационной среды образовательного учреждения. Чтобы понять ее значимость и обширность рассмотрим какие ресурсы включает в себя образовательная среда данного учебного заведения.

Электронные образовательные ресурсы:

- образовательный портал
- Web-страница преподавателя
- программные оболочки Moodle
- учебно-методический комплекс на основе кейс-технологий (на бумажных носителях)
- учебно-методический электронный комплекс по специальности
- более 50 электронных учебников по дисциплинам
- система организации самостоятельной работы студентов в электронной библиотеке
- междисциплинарный учебно-методический электронный комплекс по компетенциям
- электронные учебники по компетенциям

- практическое обучение в корпоративных учебно-производственных центрах
- система сертификации
- мониторинг (система оценки знаний, умений, навыков)

Доступ ко всем ресурсам осуществляется через локальную(корпоративную) сеть образовательного учреждения. Таким образом все электронные ресурсы напрямую зависят от развитой структуры сети и ее оснащения.

Администрированием сети и разграничением прав пользователей занимается технический отдел колледжа. Политика безопасности домена предписывает пользователям регулярно изменять свои пароли, контролирует не повторяемость и непохожесть паролей.

В локальной сети колледжа для сотрудников доступны шаблоны различных документов, так же сеть используется для обмена текущими документами. Для этого используются общие папки Windows. Доступ к общим папкам ограничен в зависимости от статуса сотрудника. Сотрудник колледжа может изменять хранящиеся в них документы только в том случае, если у него есть доступ к данной и папке, и он зашел под той ученой записью, в которой был создан данный документ.

Сотрудники колледжа имеют доступ в Интернет через шлюз в корпоративной сети. С помощью электронной почты ведётся обмен документами с другими образовательными организациями и Министерством образования Челябинской области.

Локальная сеть рассчитана на одновременную работу 768 компьютеров. (Высокоскоростная глобальная сеть (пакет 20 000 Мб в месяц). 70% учебных площадей оснащено компьютерной и коммуникационной техникой (в т.ч. 450 рабочих мест электронной библиотеки) 150 мест Internet в общежитии);

Предоставление доступа к Internet осуществляется по технологии ADSL, позволяющая получать скорость потока данных в пределах от 1,5 Мбит/сек, до 8 Мбит/сек. Технология ADSL позволяет телекоммуникационным компаниям

предоставлять частный защищенный канал между пользователем и провайдером. Технология ADSL – самая распространенная и востребованная услуга на настоящий момент.

Аппаратное оснащение локальной сети включает в себя:

- компьютеры (серверы и рабочие станции)
- сетевые платы (адаптеры)
- каналы связи
- специальные устройства, поддерживающие функционирование сети (маршрутизаторы, концентраторы, коммутаторы)

В основе сети колледжа лежит смешанная топология. В сеть объединены несколько подсетей, отдельно для студентов и администрации колледжа. Это обеспечивает дополнительную защиту информации.

Локальная сеть имеет централизованное управление, которое осуществляется с помощью серверов. Персональные компьютеры в структуре данной сети выполняют роль клиента. Благодаря такому строению можно настроить надежную политику безопасности, а также в какой-то мере предотвратить угрозу несанкционированного доступа к конфиденциальным данным.

Как и любая другая сеть локальная сеть колледжа имеет протоколы передачи данных или сетевые протоколы.

Корпоративная сеть колледжа построена на принципах протоколов TCP/IP.

Сетевой протокол - это четко определенный набор правил и соглашений для взаимодействия одинаковых уровней сети.

Протоколы TCP/IP - набор широко используемых в Интернете сетевых протоколов, поддерживающий связь между объединенными сетями, состоящими из компьютеров различной архитектуры и с разными операционными системами. Протокол TCP/IP включает в себя стандарты для

связи между компьютерами и соглашения о соединении сетей и правилах маршрутизация сообщений. Собственно этот протокол состоит из двух протоколов:

- TCP (Transmission Control Protocol) – протокол, отвечающий за формирование и отправку пакетов.
- IP (Internet Protocol) – маршрутизируемый протокол семейства TCP/IP, отвечающий за IP-адресацию, маршрутизацию, а также за разбиение на сегменты и повторную сборку пакетов IP.

Для защиты корпоративной сети используются следующие средства:

1. Межсетевые экраны - локальное или функционально распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и/или выходящей из автоматизированной системы. По определению межсетевые экраны служит контрольным пунктом на границе двух сетей. В самом распространенном случае эта граница лежит между внутренней сетью организации и внешней сетью, обычно сетью Интернет. Однако в общем случае, межсетевые экраны могут применяться для разграничения внутренних подсетей корпоративной сети организации.

2. Антивирусная защита. Антивирусная защита имеет комплексный характер — устанавливается на компьютеры пользователей, а также в качестве системы мониторинга и контроля обновлений на сервера.

3. Своевременные обновления программного обеспечения. Данная мера позволяет своевременно закрыть ставшие известными уязвимости в программном обеспечении и избежать появления вирусов, а также не стать жертвой хакерских атак.

4. Использование брандмауэра. Это программа, которая следит за сетевыми соединениями и принимает решение о разрешении или запрещении новых соединений на основании заданного набора правил.

Выводы по Главе 2

В ходе работы над данной главой была проанализирована система обеспечения безопасности Южно-Уральского Государственного колледжа.

Анализ системы безопасности показал:

1. Колледж имеет довольно обширную корпоративную сеть. В нее объединены все компьютеры, имеющиеся в распоряжении колледжа, а также сервера для хранения и обработки информации.
2. Политика безопасности колледжа несовершенна. В корпоративной сети колледжа нет полноценного мониторинга уязвимостей и ошибок, а также нет полноценного контроля доступа к сети.
3. Система безопасности не обладает необходимыми инструментами для защиты корпоративной сети колледжа.

Таким образом корпоративная сеть нуждается в усовершенствовании системы безопасности. Повысить безопасность возможно организовав централизованный мониторинг за событиями в корпоративной сети колледжа.

ГЛАВА 3 СОВЕРШЕНСТВОВАНИЕ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИИ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

3.1. Выявление угроз, уязвимостей и рисков в системе защиты информации колледжа.

Существующая система обеспечения информационной безопасности в колледже имеет уязвимости.

Одним из уязвимых мест в системе безопасности можно назвать сотрудников колледжа и программно-аппаратные средства. В частности в колледже: не выполняется резервное копирование данных на персональных компьютерах сотрудников колледжа - при отказах оборудования некоторые важные данные могут быть потеряны; не выполняется обновление операционной системы MS Windows и использующегося ПО, что может привести к несанкционированному доступу к хранящейся на ПК информации или её повреждению из-за ошибок в ПО; доступ сотрудников к ресурсам Интернета не контролируется, из-за этого может произойти утечка данных; деловая электронная переписка ведётся через Интернет по незащищённым каналам, сообщения электронной почты хранятся на серверах почтовых служб в Интернете; некоторые сотрудники имеют недостаточные навыки работы с автоматизированными системами, используемыми в колледже, что может привести к появлению в системе неверных данных; отсутствуют нормативные документы по безопасности.

В отношении корпоративной сети также имеются проблемы обеспечения безопасности. Сеть защищают стандартными методами: антивирусы, брандмауэры, программы для защиты от спама.

При этом не существует централизованной системы мониторинга, которая позволила бы получать оперативную информацию о состоянии сети, проблемах и отказах, попытках несанкционированного доступа. Все данные о неполадках в сети системные администраторы получают от пользователей, то есть практически случайным образом. Данная ситуация так же влияет на сбор

статистики по работе корпоративной сети, ее надежности и отказоустойчивости. То есть по факту о состоянии сети имеются только разрозненные и устаревшие данные, на основании которых произвести анализ надежности системы безопасности производить тяжело, а говорить о ее объективности и вовсе невозможно.

3.2. Мероприятия и средства по совершенствованию системы информационной безопасности колледжа. Внедрение программного обеспечения с целью повышения информационной безопасности.

Главной проблемой в обеспечении безопасности информационного пространства колледжа является безопасность корпоративной сети. Необходимо принять меры для повышения безопасности.

Самым эффективным средством для повышения безопасности корпоративной сети является мониторинг. Сбор сведений о состоянии сети в режиме реального времени поможет значительно повысить скорость обнаружения неполадок и сократит время на их устранение. Также мониторинг поможет собрать статистику неисправностей и уязвимостей, что позитивно скажется на повышении безопасности сети в будущем, так как можно будет подобрать наиболее эффективные методы борьбы с ними.

Для того, чтобы подобрать наиболее эффективную систему мониторинга сети необходимо очертить круг задач, которые необходимо решить:

- Необходимо отслеживать все процессы, происходящие в сети
- Оперативно отслеживать аномальную активность в сети
- Оперативно получать уведомления о сбоях в работе сети
- Оперативно получать информацию о состоянии каждого из элементов сети.

Так же необходимо отметить, что предпочтительнее будет именно та система, для внедрения которой не потребуется дополнительного оборудования.

Опираясь на поставленные требования, был изучен рынок продуктов мониторинга сети.

Самые распространенные продукты для мониторинга сети: Nagios, PRTG Network Monitor, Cacti, Zabbix.

Для того, чтобы понять какая система наиболее подходит для внедрения в данном случае необходимо провести сравнительный анализ данных систем.

Nagios

Nagios – это продвинутое решение для мониторинга, управление которым основано на веб-интерфейсе. Он отнюдь не прост в освоении, однако, благодаря своему довольно большому интернет-сообществу и хорошо проработанной документации, может быть освоен за несколько недель.

С помощью Nagios системные администраторы получают возможность удаленно регулировать объем нагрузки на пользовательское или вышестоящее в сетевой иерархии оборудование (коммутаторы, маршрутизаторы, серверы), следить за степенью загруженности резервов памяти в базах данных, следить за физическими показателями частей сетевого оборудования (например, температурой материнской платы, сгорание которой является одной из самых частых поломок в данной сфере) и пр.

Достоинства:

- Легко настраивается
- Большое обилие плагинов
- Бесплатный

Недостатки:

- Отсутствуют встроенный средства визуализации (кроме карты сети)
- Сложность масштабирования без использования плагинов от сторонних производителей
- Нет возможности для мониторинга производительности
- Нет возможности конфигурирования через интерфейс
- Требуется перезапуск сервера для вступления в силу изменений в конфигурации
- Каждый плагин запускается как отдельный процесс

PRTG Network Monitor

PRTG Network Monitor от Paessler AG существенно облегчает мониторинг сети за счет своевременного уведомления о любых сбоях посредством простого и удобного веб-интерфейса. Богатый набор датчиков разных типов в сочетании с возможностью подключения к любому сетевому узлу гарантирует постоянное наблюдение за состоянием сети.

Достоинства:

- Предельно прост в установке
- Самостоятельно умеет собирать информацию о сети
- Прост в эксплуатации
- Не требует каких либо установок на стороне серверов кроме настройки файрволла
- Рисует удобные и легкочитаемые графики

Недостатки:

- Работает только на серверах, где установлена ОС Windows
- Платный

Cacti

С его помощью можно контролировать большое количество различных параметров, таких как загрузку систем и сетей, с выводом всевозможных графиков. Cacti без проблем будет работать в сетях любого размера, как

маленьких, так и больших, со сложной разветвленной топологией. В качестве источника данных могут быть использованы любые внешние команды или сценарии с любыми параметрами, которые нужно собрать, реализована поддержка SNMP. Интерфейс написан на PHP, вся собранная информация сохраняется в базе данных MySQL. Распространяется Cacti по лицензии.

Достоинства:

- Прост в освоении и развертке
- Не требователен к ресурсам
- Также не нужно устанавливать ничего кроме настройки файрволла
- Множество графиков для детального мониторинга

Недостатки:

- Устаревшие методы сбора информации
- Непрезентабельный интерфейс

Zabbix

Zabbix — это полномасштабный инструмент для сетевого и системного мониторинга сети, который объединяет несколько функций в одной веб-консоли. Он может быть сконфигурирован для мониторинга и сбора данных с самых разных серверов и сетевых устройств, обеспечивая обслуживание и мониторинг производительности каждого объекта.

Достоинства:

- Широкие возможности мониторинга
- Множество триггеров, вплоть до температуры устройства
- Кроссплатформенность (Windows/Unix/Linux системы)
- Отправка данных на электронную почту и в мессенджеры (slack, telegram)
- Бесплатный

Недостатки:

- Высокие требования к аппаратной части, большая нагрузка
- Достаточно сложная первоначальная настройка
- Требует установки агента непосредственно на каждом сервере

Для решения проблемы мониторинга корпоративной сети образовательного учреждения была выбрана система мониторинга zabbix. Данная система лучше остальных подходит для решения обозначенных проблем. Программа бесплатна, исходный код ее открыт. Никаких дополнительных затрат и оборудования программа не требует. В данном случае это идеальный вариант. Рассмотрим подробнее, что представляет из себя данная система мониторинга.

Zabbix - это программное обеспечение для мониторинга многочисленных параметров сети, жизнеспособности и целостности серверов. Zabbix использует гибкий механизм оповещений, что позволяет пользователям конфигурировать уведомления основанные на e-mail практически для любого события. Это позволяет быстро реагировать на проблемы с серверами. Zabbix предлагает отличные функции отчетности и визуализации данных основанные на данных истории. Это делает Zabbix идеальным для планирования мощности.

Система мониторинга Zabbix – это универсальное решение для сетевого мониторинга с открытым исходным кодом, которое может быть сконфигурировано под отдельные сетевые модели. В основном, оно предназначено для систем, которые обладают многосерверной архитектурой (в частности, Zabbix интегрируется с серверами Linux/FreeBSD/Windows).

Данное приложение позволяет одновременно управлять сотнями сетевых узлов, что делает его крайне эффективным инструментом в организации работы сисадминов, работающих на крупномасштабных предприятиях. Для развертывания Zabbix в своей локальной сети вам потребуется либо запустить программных агентов (демонов), либо использовать SNMP-протокол (или

другой протокол для защищенного удаленного доступа); а для управления придется освоить веб-интерфейс на PHP.

Кроме того, это ПО предоставляет полноценный набор инструментов для отслеживания состояния аппаратной части сети. Отметим, что для того, чтобы в полной мере ощутить все преимущества данного решения, вашему системному администратору придется обладать хотя бы базовыми знаниями языков Perl или Python (или каких-либо других языков, которые можно совместно использовать с Zabbix).

Система состоит из четырёх основных компонентов: Сервер мониторинга, который собирает и обрабатывает данные от всех агентов. Прокси сервер, выполняющий те же функции, но с последующей отправкой на центральный сервер. Веб-интерфейс для мониторинга. Агент, собирающий данные на физическом сервере. Для работы необходима одна из нескольких возможных вариантов баз данных, которая должна быть предварительно настроена (это происходит автоматически, с помощью готовых скриптов): MySQL, Oracle, PostgreSQL, SQLite, IBM DB2.

Применение системы zabbix. Внедрение

Для внедрения данного программного продукта необходим установочный файл, который можно скачать на сайте производителя продукта. Лицензии для данного продукта, как уже было сказано — не требуется.

Необходимо определить сервер на который будет устанавливаться система мониторинга. В корпоративной сети есть сервер, который имеет доступ ко всем подсетям корпоративной сети. Его мощности достаточно, чтобы установить систему мониторинга.

Установка особого внимания не требует, так как программа мониторинга устанавливается как и любая другая программа. Доступ к программе осуществляется через браузер. Достаточно ввести в командную строку адрес: http://localhost/

Особое внимание необходимо уделить настройке. Система очень гибкая и настраивается под каждый конкретный случай внедрения.

Чтобы понимать, как правильно настроить программу необходимо понимать принципы ее работы.

Основная логическая единица — узел сети или хост(host). Под хостом подразумевается сервер. Связь с сервером в программе осуществляется через IP-адрес или dns(на выбор).

Каждый узел имеет несколько элементов данных — параметров, за которыми ведется мониторинг. Еще одним основным понятием системы является триггер. Триггеры — это настраиваемые правила. Они активируются при неполадках в сети и сигнализируют об авариях системному администратору. При этом в зависимости от настройки это может быть звуковое или световое уведомление. При необходимости можно настроить отправку уведомлений о неполадках на почту. Но система мониторинга настолько самостоятельна, что может самостоятельно попытаться устранить неполадку, если сценарий ее устранения настроен.

Начнем первичную настройку системы мониторинга. При первом входе система требует логин и пароль. Стандартно логин/пароль admin/zabbix.

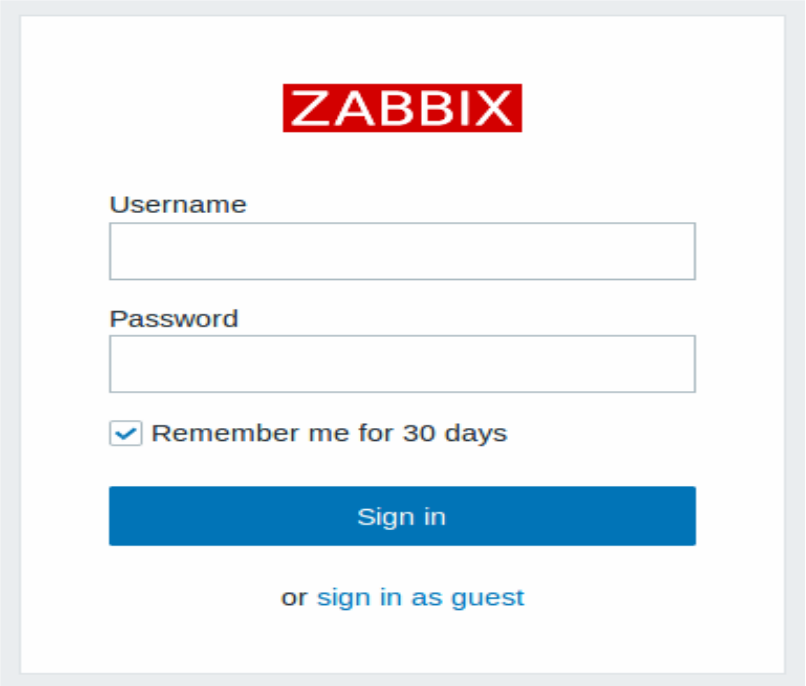


Рис. 2 Экран приветствия

Под этим паролем вход осуществляется с правами Супер-Администратора. Это понятие в системе мониторинга означает, что у данного пользователя нет никаких ограничений в системе. Пользователь имеет доступ ко всем меню, настройкам и группам. Только данный пользователь имеет право добавлять новых пользователей и разграничивать права доступа.

Также в системе существуют понятия Администратор и пользователь. Соответственно Администратор может производить настройку системы, но при этом имеет доступ только к тем узлам сети, которые разрешены при настройке прав. Пользователь же имеет право только на мониторинг узлов сети. Доступ так же предоставляется в разрезе узлов сети. Соответственно назначаем администраторам права Администратора системы, а старшему администратору оставляем права Супер-Администратора.

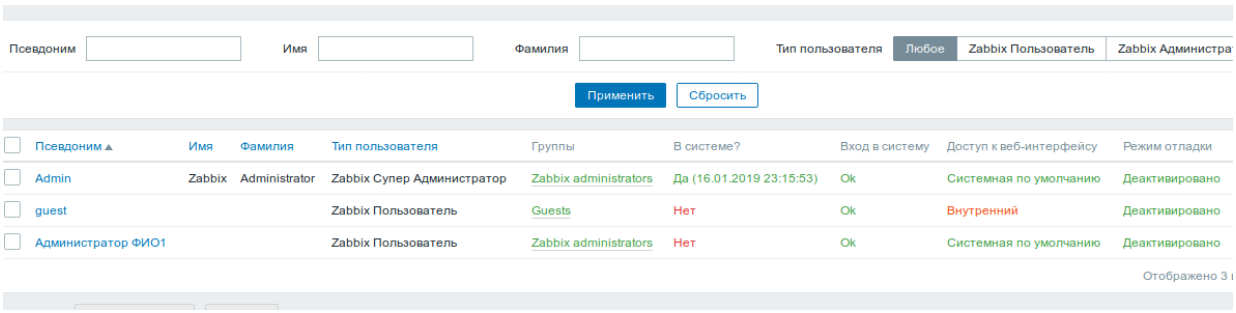


Рис. 3 Настройка пользователей

Для дальнейшей работы необходимо, чтобы стали видны элементы сети. Это можно сделать двумя способами: вручную добавить все узлы сети, и воспользоваться автоматическим обнаружением. Так как сеть обширная использован вариант автоматического обнаружения. Для этого заданы правила обнаружения и добавления в общую сеть всех устройств. Правила настроены таким образом, что обнаружение устройств в сети производится с определенным интервалом времени — 1 час. Это значит, что каждый час система опрашивает свое окружение на предмет обнаружения новых устройств и автоматически включает их для себя в структуру сети.

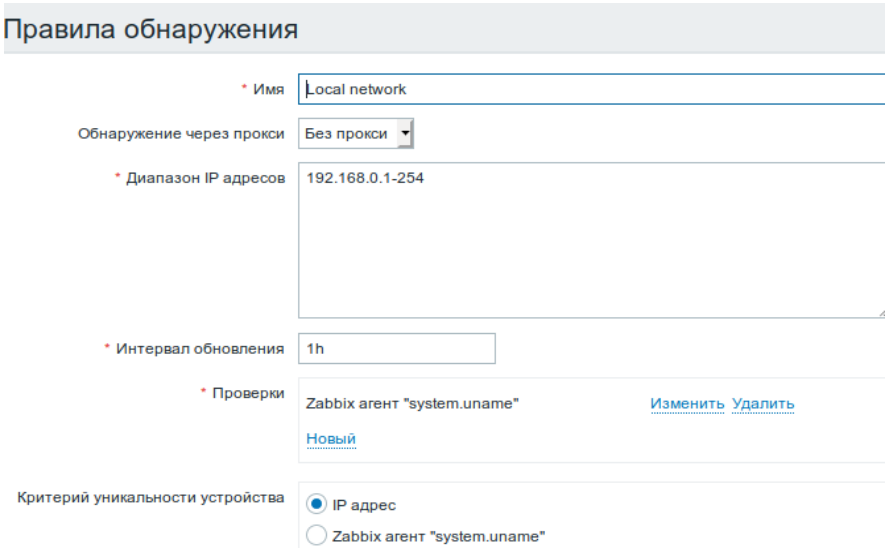


Рис. 4 Правило обнаружения

Но обнаружить устройства мало. Необходимо добавить их в систему для возможности мониторинга. Для этого настраиваем правило добавления обнаруженных устройств в сеть.

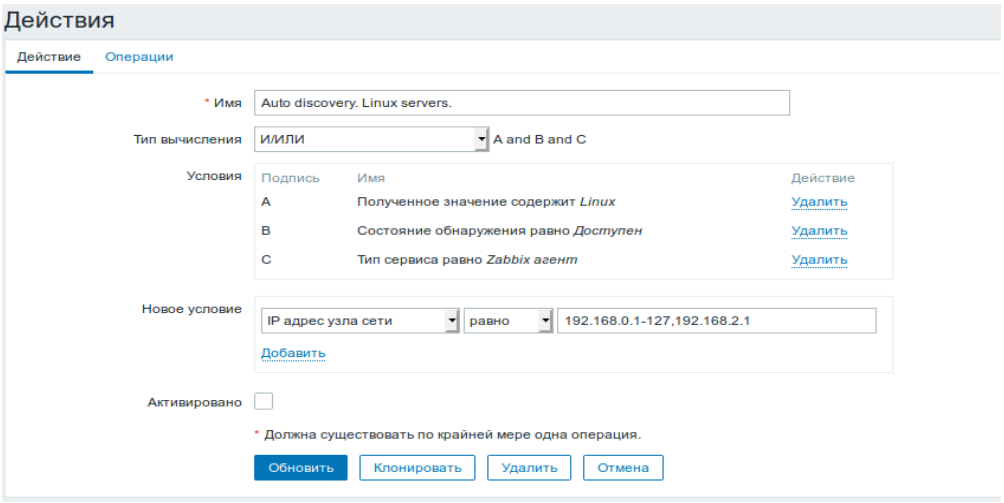


Рис. 5 Правило обнаружения

Одной из задач, поставленных в ходе данной работы, является оперативное получение данных о состоянии сети и возникающих неполадках. Поэтому один из важных этапов настройки системы мониторинга — настройка отправки оповещений.

Оповещения могут приходить различными способами: по смс, по электронной почте, jabber, скрипты для оповещений.

Так как систему обслуживает небольшое число человек, то целесообразно настроить оповещения по электронной почте.

При установке системы автоматически создаются варианты оповещений. Необходимо только задать настройки.

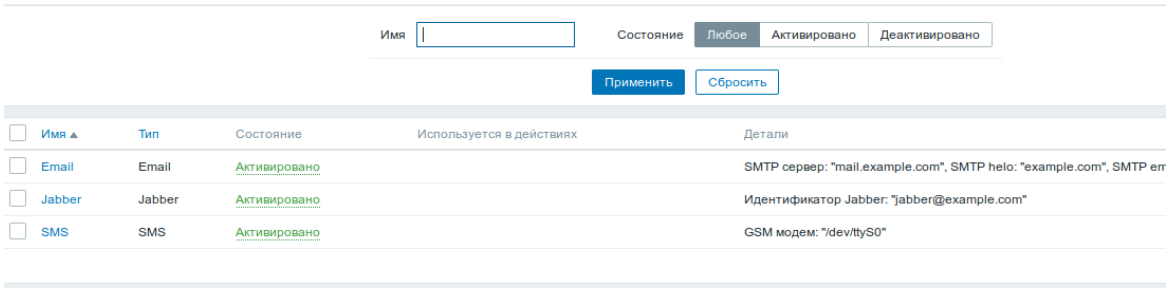


Рис. 6 Стандартные настройки оповещений

Для того, чтобы настроить оповещения по электронной почте необходимо назначить адрес отправки и адрес получения.

Адрес отправки задается в меню оповещения.

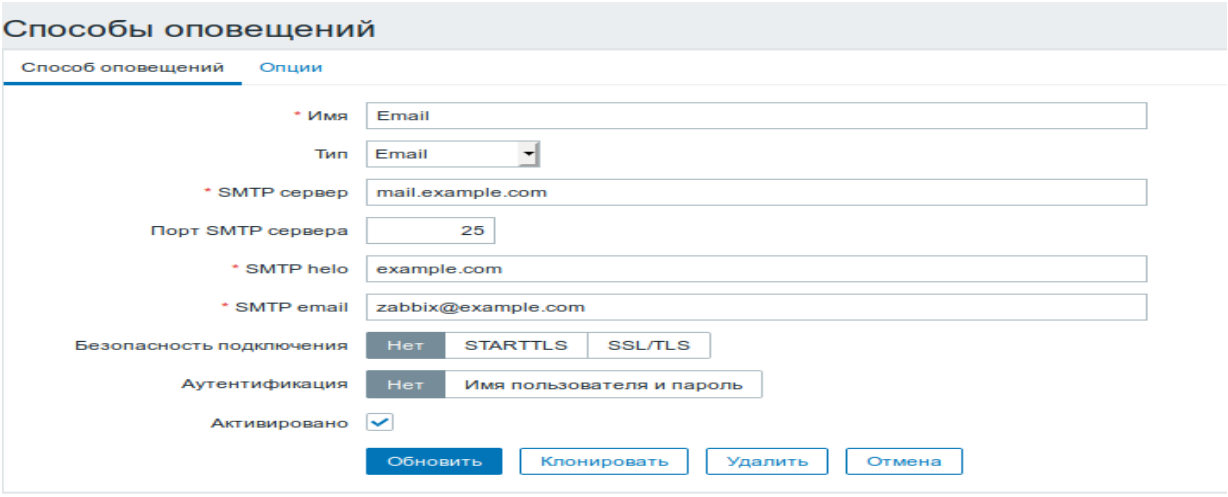


Рис.7 Настройка адреса отправки

Настройка адреса получения производится в настройках пользователя. Оповещения можно настроить таким образом, чтобы при сбое в определенных узлах сети сообщение приходило только администратору, ответственному за этот участок, нескольким администраторам (например, дублировалось старшему администратору), либо приходило всем без исключения. Возможно, настроить время оповещений. Так, например, оповещения могут приходить только в рабочее.

Так же при настройке адреса можно выбрать какие оповещения будут приходить: важные, средней степени важности или все.

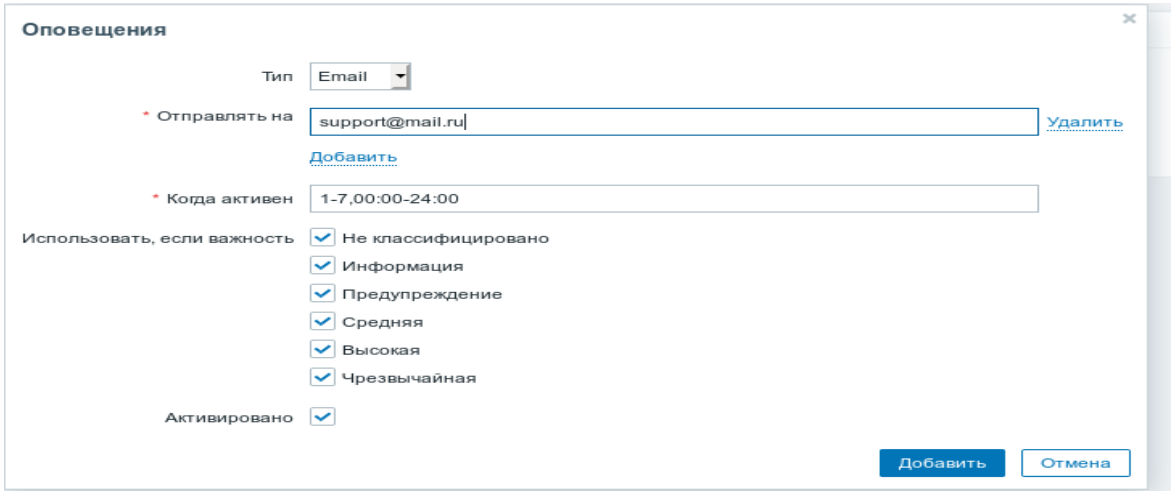


Рис. 8 Настройка почты получателя

Таким образом решается задача оперативного оповещения персонала о событиях в сети.

Теперь необходимо настроить оповещения. Оповещения могут быть настроены для любого сбоя, неполадки или события в сети (например, успешное окончание создания резервной копии. Для создания оповещения необходимо составить сообщение об ошибке (чтобы сразу было понятно в каком узле произошло данное событие), а также определить кому и каким способом будет приходить оповещение.

Первоначальные настройки сделаны. Теперь важно правильно настроить критерии мониторинга. Чтобы отслеживать состояние узла сети необходимо связать его с системой мониторинга. Это можно сделать двумя способами: через агента и методом простых проверок.

Система мониторинга имеет структуру клиент-сервер. Все вышеописанные настройки производились на сервере zabbix. Для того, чтобы серверу стали видны узлы сети можно установить на каждый из них zabbix-агент. При такой схеме сервер опрашивает агента и таким образом получает информацию об устройстве и его функционировании.

Но корпоративная сеть колледжа обширна и ставить агенты на каждое устройство нецелесообразно. Да и на такие узлы сети как маршрутизаторы агент не всегда можно поставить. Поэтому для опроса узлов сети будет

использоваться технология простых проверок. Эта технология основана на протоколе SNMP.

SNMP (Simple Network Management Protocol) - это простой протокол сетевого управления или протокол управления устройствами в IP-сетях на основе TCP/UDP. SNMP предоставляет данные для управления устройствами сети в виде переменных, которые описывают конфигурацию данного оборудования. Эти переменные могут быть запрошены или заданы (если это позволяет оборудование и его конфигурация) управляющими приложениями. В самом протоколе SNMP не определено какая информация заложена в переменных. Для этого SNMP использует базу управляющей информации (базу MIB). Базы MIB описывают структуру управляемых данных и информацию, заложенную в переменных. MIB имеет иерархическую структуру пространства имен, содержащие идентификаторы объектов (OID). Каждый OID определяет переменную, которая может быть считана или установлена с помощью SNMP.

Вернемся к настройке критериев мониторинга. Необходимо настроить систему так, чтобы она отвечала тем задачам, которые были поставлены при ее внедрении.

Для этого в системе есть такое понятие как триггеры. Триггер - это правила по которым отслеживается состояние узла сети.

Одним из важных критериев целостности и работоспособности сети является доступность ее элементов. И в первую очередь необходимо создать шаблоны, отслеживающие доступность сети. Для этого создается шаблон данных куда входит элемент данных(отслеживающий нужное событие) и триггер(реакция на событие)

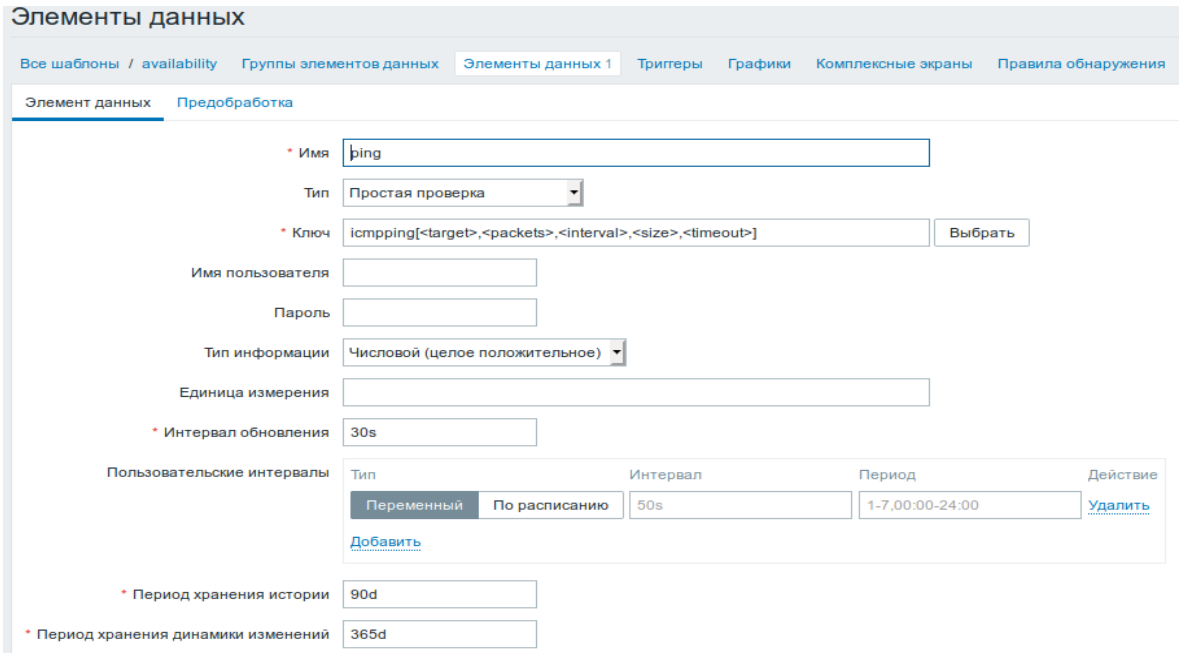


Рис. 9 Элемент отслеживания состояния

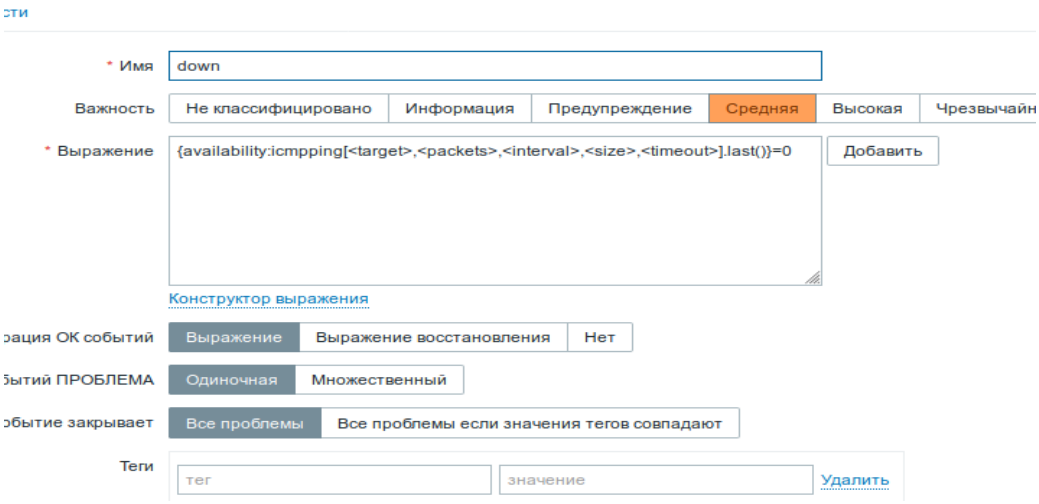


Рис. 10 Триггер состояния

Подобным образом настраивается контроль основных узлов сети и при проблемах с ними будет выведено сообщение (в нашем случае отправлено на электронную почту), где будет указан узел сети и проблема, возникшая с ним.

Такова первоначальная настройка мониторинга элементов сети, таких как сервера и пк пользователей. Но есть не менее важные узлы сети — маршрутизаторы, порты, то есть все то оборудование, которое отвечает за работу корпоративной сети. Их мониторинг не менее важная задача.

Чтобы настроить мониторинг портов необходимо создать новый узел сети только уже с параметрами устройства.

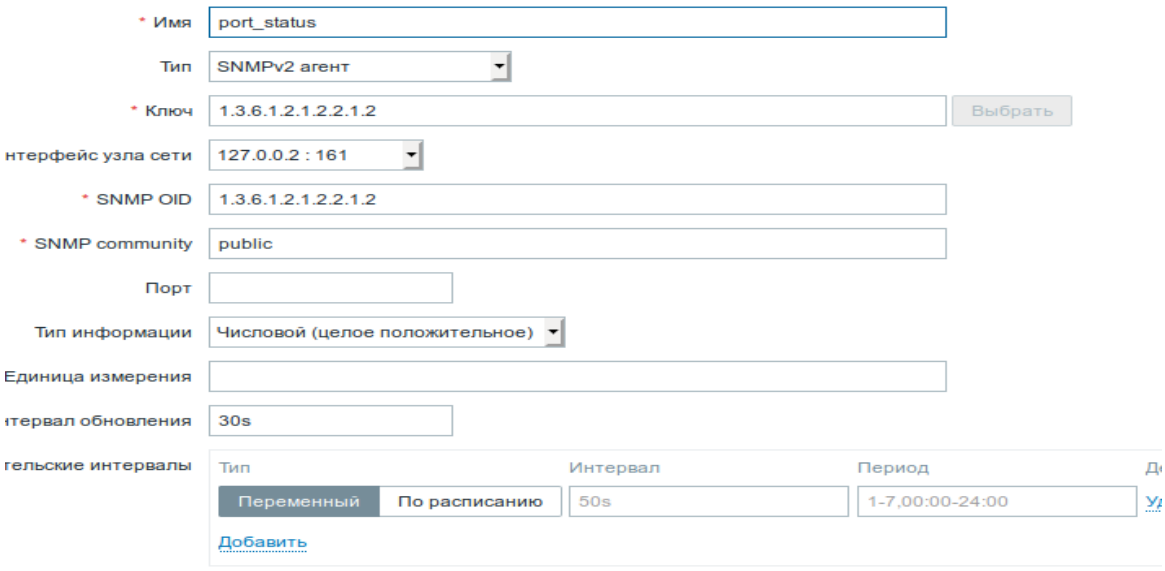


Рис. 11 Параметры оборудования

Так же, как и для отслеживания активности в сети необходимо настроить триггер.

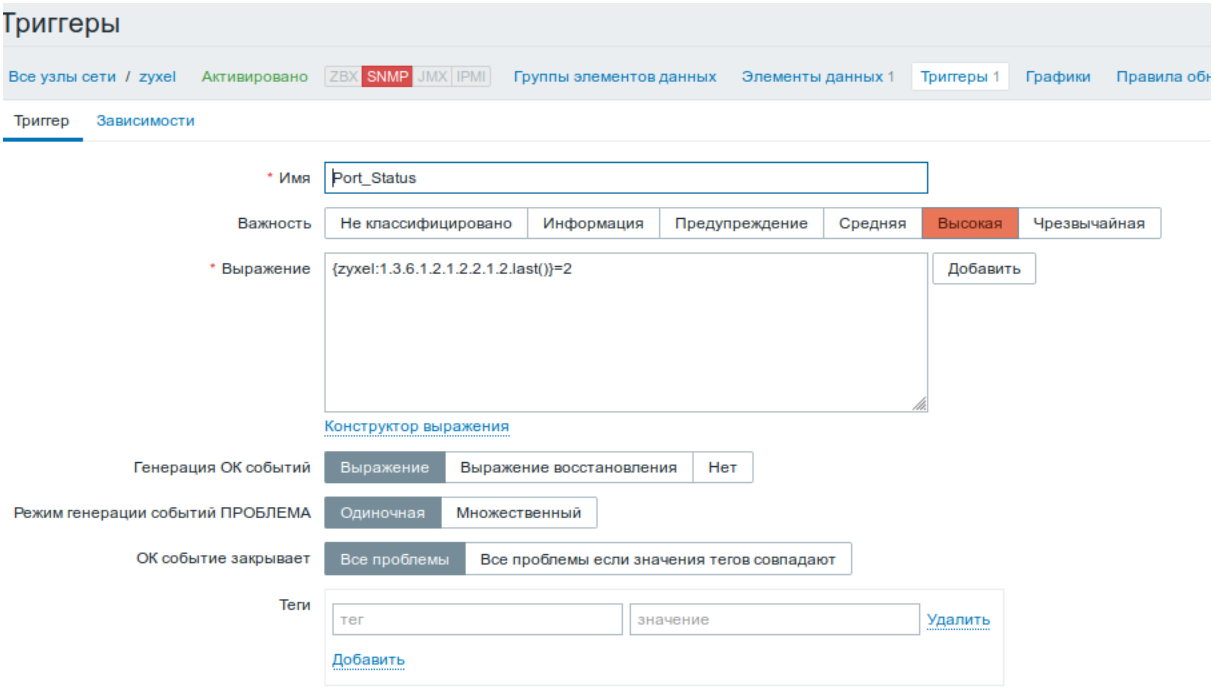


Рис. 12 Триггер для мониторинга состояния

Подобным образом произведена настройка реагирования на аномальную активность в сети. За основу были взяты параметры загрузки оборудования в среднем недельной давности — это относительно нормальный режим работы для всех показателей системы. Теперь если показатели будут превышены на

определенный порядок — система мониторинга сообщит об этом системным администраторам.

Так выглядит первоначальная настройка мониторинга для круга задач, ставших целью данного исследования. Но необходим так же визуальный мониторинг в режиме реального времени. Для этого настроим карту сети.

Карта сети — это схема узлов сети, которая соответствует реальной сети и имеет тот же набор элементов. Проще говоря, карта сети — это схема на которой наглядно представлена сеть.

Существует два типа карт сети: публичные и приватные.

Публичные карты сети видимы всем пользователям, однако, эти пользователи должны иметь как минимум права на чтение по крайней мере одного элемента карты сети, чтобы её увидеть. Публичные карты можно редактировать в случае, если пользователь/группа пользователей имеет права чтения-записи к этой карте и по крайней мере права чтения всех элементов соответствующей карты, включая триггеры в связях.

Приватные карты сети видны только своим владельцам и пользователям/группам пользователей с общим доступом к этой карте сети, которым поделился владелец. Обычные пользователи (не Супер-Администраторы) могут предоставлять общий доступ только тем группам и пользователям, которым они принадлежат сами. Пользователи уровня Администратора могут видеть приватные карты сети независимо от того, являются ли они владельцами или принадлежат списку пользователей с общим доступом. Приватные карты может редактировать владелец карты и пользователь/группа пользователей с правами чтения-записи этой карты сети и по крайней мере с правами чтения всех элементов соответствующей карты, включая триггеры в связях.

В рамках внедрения была создана публичная карта. Это целесообразно в данном случае так как количество сотрудников, обслуживающих корпоративную сеть мало и обязанности не распределены для каждого отдельного сегмента сети.

Карта имеет имя, ширину и высоту. Также можно задать детализацию элементов (узел сети, группа узлов сети и прочее), детализацию событий, важность событий. В зависимости от настроек на карте будут отображаться события, например с пометкой важное.

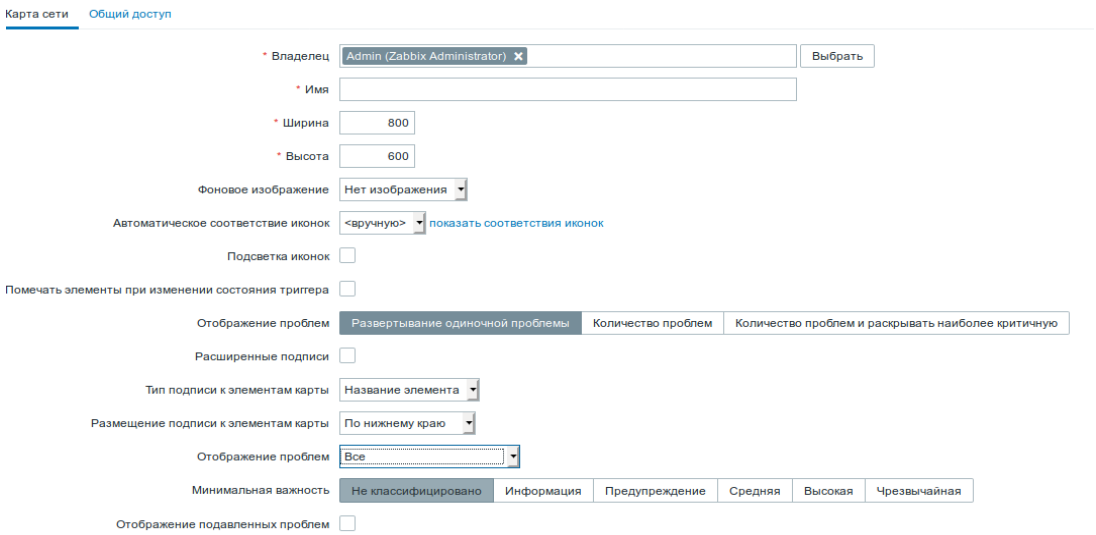


Рис. 13 Создание карты сети

После того, как карта создана необходимо расположить на ней элементы сети. В зависимости от настроек детализация карты может быть различной: узлы корпоративной сети, подсеть, пользовательские компьютеры.

В данном случае карта отображает основные узлы корпоративной сети, для которых была произведена настройка мониторинга.

Процесс создания карты сети напоминает компьютерную игру. Элементы сети представлены в виде картинок — изображений различного оборудования.

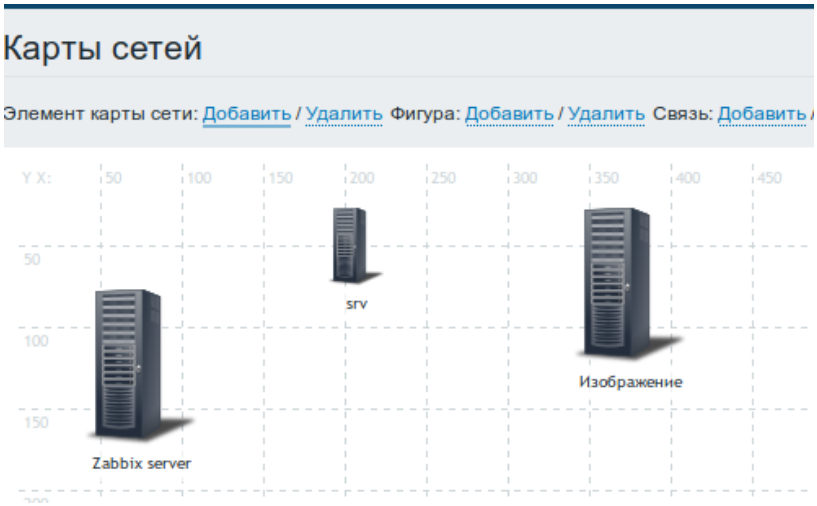


Рис. 14 Настройка карты сети

Для наглядности можно связать элементы сети. То есть продемонстрировать топологию сети. Всю корпоративную сеть вместить на карту проблематично, поэтому приведем пример фрагмента карты.

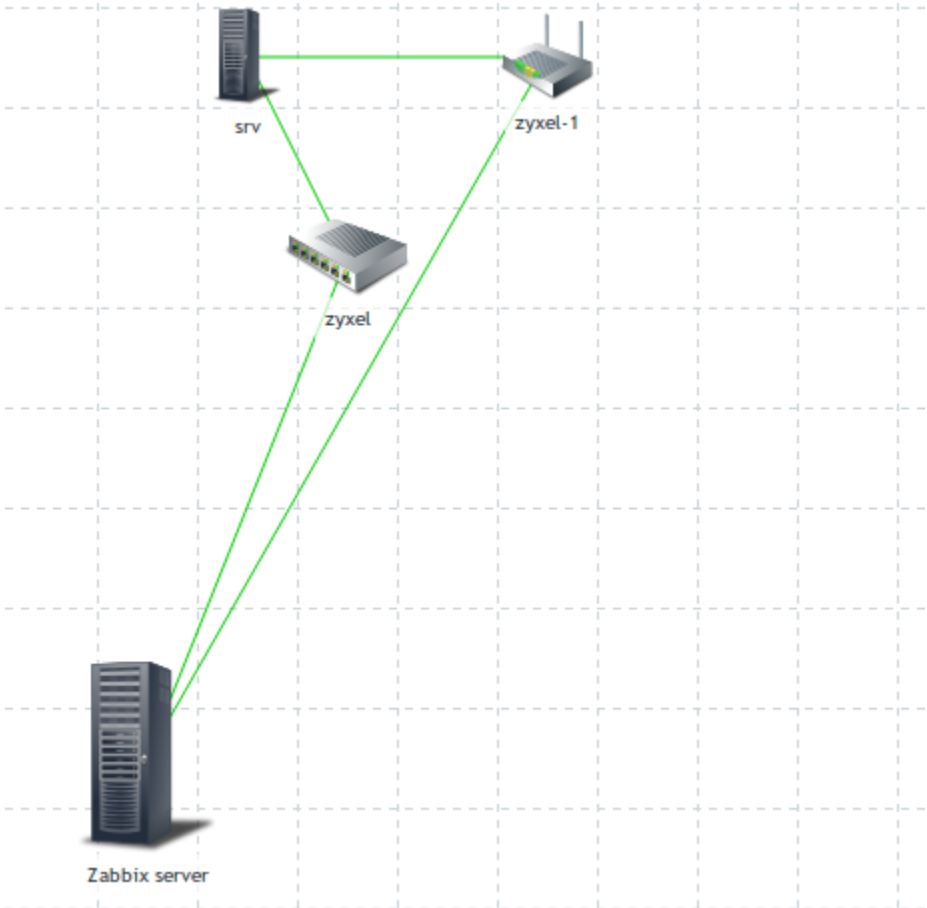


Рис. 15 Фрагмент карты сети

Для визуального отслеживания состояния сети в режиме реального времени был настроен комплексный экран — отчет, куда можно добавить нужные графики. Для нашей задачи комплексный экран включает в себя графики Обзор триггеров (информация о срабатывании), Информация о системе, Информация о доступности узлов сети.

Для мониторинга всей корпоративной сети колледжа были созданы несколько карт: карты подсетей и карта триггеров, чтобы отслеживать проблемы по причине их возникновения.

Отслеживать проблемы и неполадки сети можно и стандартными отчетами системы мониторинга.

Система мониторинга хранит все данные, поэтому отчеты можно строить не только на текущее время, но и за неделю, месяц, год. Это позволяет получать статистику о работе системы, ее состоянии. На основании этих данных можно распланировать календарь профилактики узлов сети и своевременно заменить их.

Также с помощью отчетов можно предоставить информацию для разбора уже произошедшей ситуации, понять, что послужило причиной и как не допустить в будущем повторения ситуации. Так, например, можно отследить какие триггеры чаще всего срабатывают и понять почему.

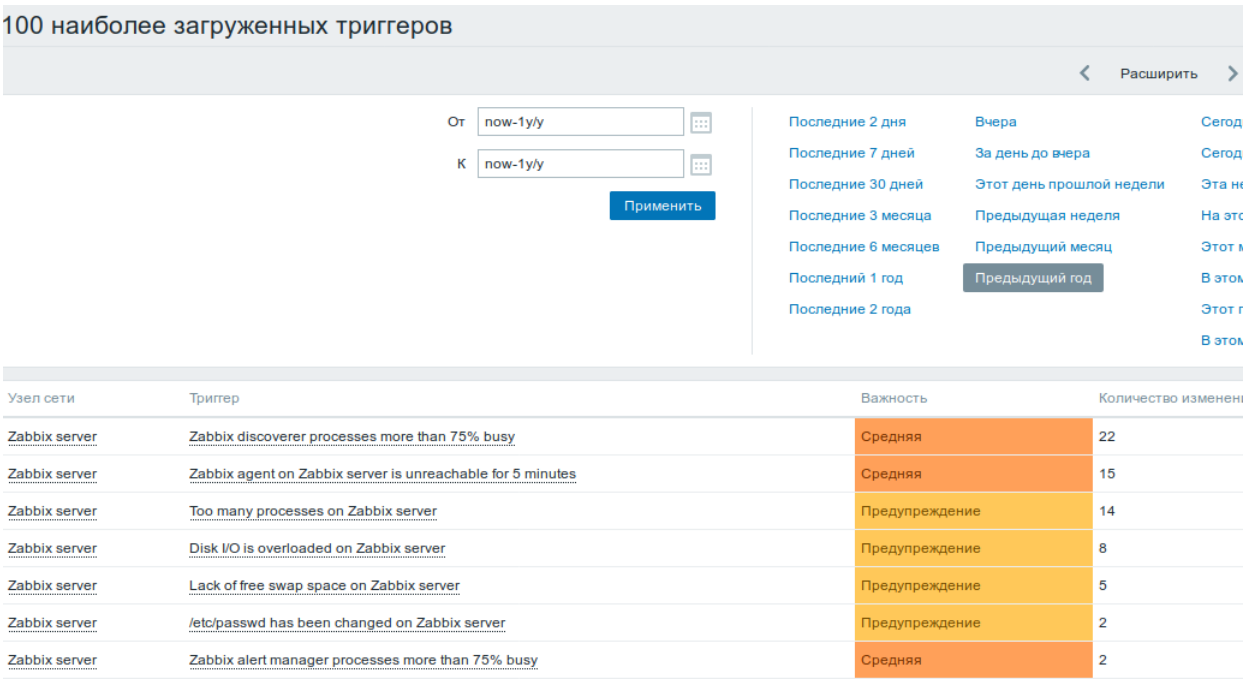


Рис. 16 Отчет отслеживания активности триггеров

Так как была произведена настройка оповещений, доступен отчет, который показывает какому пользователю когда и сколько раз приходили оповещения. Это очень удобно так как можно не хранить оповещения на электронной почте. И даже при сбое в электронной почте с потерей всех данных можно будет восстановить историю оповещений с помощью системы мониторинга.

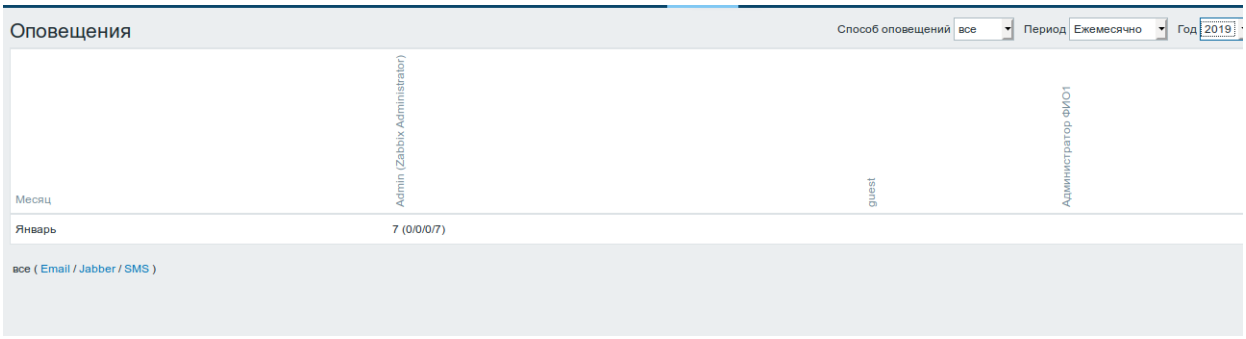


Рис 17. Отчет статистики оповещений

Есть возможность отслеживать не только состояние сети, но и состояние самой системы мониторинга. Это очень важно, так как если система будет

давать сбои реальное положение дел в корпоративной сети колледжа оценить станет невозможным.

Правильной работе системы мониторинга может помешать критическая загрузка сервера, где она установлена. Существуют отчеты для оценки различных параметров сервера. В большинстве своем они представлены в виде графиков и диаграмм для большей наглядности.

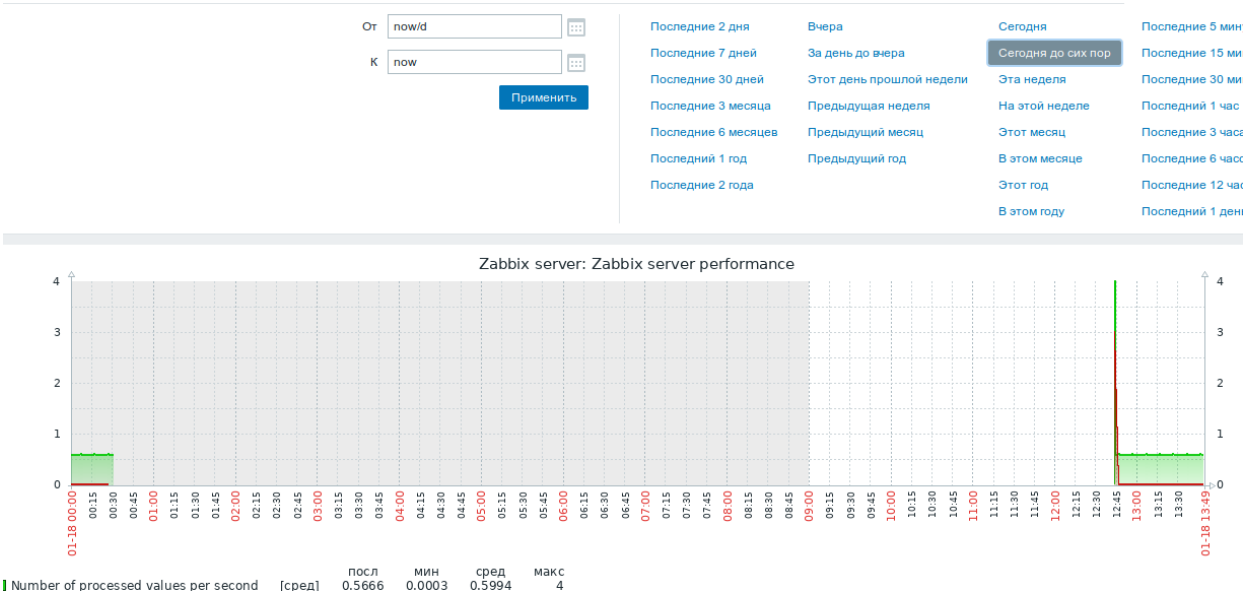


Рис. 18 Отчет загрузки сервера

В ходе внедрения были произведены установка системы мониторинга, ее первоначальная настройка, проверена работоспособность системы.

Персоналу отдела поддержки выданы учетные данные для входа в систему с определенным набором прав. Права назначены с учетом занимаемой должности и обязанностей, выполняемых тем или иным сотрудником. За начальником отдела закреплены права Супер-Администратора и только он может вносить изменения в ключевые настройки системы, добавлять пользователей, изменять уже существующих.

3.3. Оценка эффективности мероприятий по совершенствованию информационной безопасности в организации профессионального обучения

Эффективность обеспечения информационной безопасности будет низкой при отсутствии средств сбора, анализа и хранения информации о состоянии информационной среды и централизованного управления всеми ее составляющими.

Политике информационной безопасности организации должен соответствовать как каждый элемент информационной среды, так и сама среда в целом.

Для повышения уровня информационной безопасности необходимо иметь инструменты для отслеживания и фиксации возникающих проблем. Особенно остро нуждаются в таких инструментах образовательные учреждения. Наличие множества компьютерных аудиторий, а также обширной корпоративной сети требует ответственного подхода к обеспечению безопасности информационной среды.

В рамках данной работы были проанализированы состояние информационной среды колледжа, политика безопасности. На основании анализа выявлены проблемные места и предприняты меры по совершенствованию системы информационной безопасности колледжа.

Самым уязвимым местом была признана корпоративная сеть колледжа из-за отсутствия средств для централизованного сбора и анализа информации о ее состоянии.

Было решено внедрить систему централизованного мониторинга zabbix для отслеживания событий в сети, а также оповещения сотрудников о неисправностях и важных событиях.

За время практики были осуществлены следующие мероприятия:

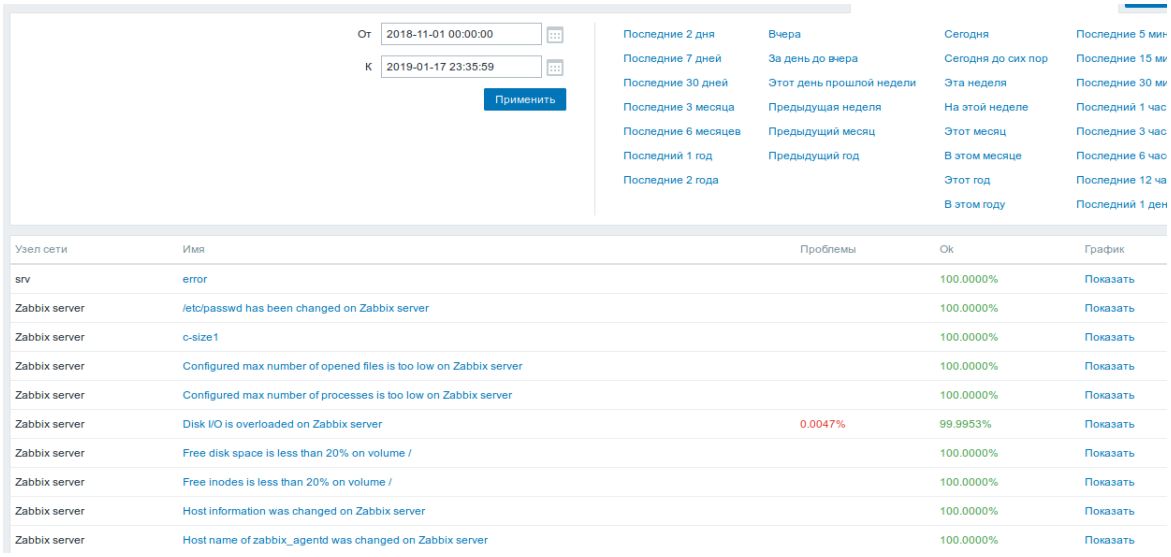
1. Анализ корпоративной сети и выявление недостатков ее мониторинга

2. Анализ средств, позволяющих устранить недостатки в обеспечении безопасности корпоративной сети
3. Проведена подготовка в внедрению: проанализировано техническое обеспечение сети, ее мощности, выбрана техническая основа внедрения
4. Внедрен мониторинг сети
5. Произведена начальная настройка системы мониторинга, определены права пользователей.
6. Произведено обучение персонала
7. Система мониторинга протестирована в рабочем режиме

Тестирование системы показало, что выбор системы мониторинга был удачным. Система решила ряд поставленных задач и стала именно тем инструментом, который повысил информационную безопасность корпоративной сети.

Персонал, обслуживающий сеть получает своевременные уведомления о проблемах сети посредством оповещений. В режиме реального времени стало возможным отследить состояние сети, увидеть сбой или неполадку.

Также стало возможным собирать и анализировать статистику работоспособности сети. Например, отчет о доступности сети показывают существуют ли проблемы с доступностью узла сети.



Узел сети	Имя	Проблемы	Ok	График
srv	error		100.0000%	Показать
Zabbix server	/etc/passwd has been changed on Zabbix server		100.0000%	Показать
Zabbix server	c-size1		100.0000%	Показать
Zabbix server	Configured max number of opened files is too low on Zabbix server		100.0000%	Показать
Zabbix server	Configured max number of processes is too low on Zabbix server		100.0000%	Показать
Zabbix server	Disk I/O is overloaded on Zabbix server	0.0047%	99.9953%	Показать
Zabbix server	Free disk space is less than 20% on volume /		100.0000%	Показать
Zabbix server	Free inodes is less than 20% on volume /		100.0000%	Показать
Zabbix server	Host information was changed on Zabbix server		100.0000%	Показать
Zabbix server	Host name of zabbix_agentd was changed on Zabbix server		100.0000%	Показать

Рис. 19 Отчет о доступности узлов сети

На рисунке видно, что один из узлов имел проблемы с доступностью. Из отчета можно построить график, который будет показывать когда возникала проблема.

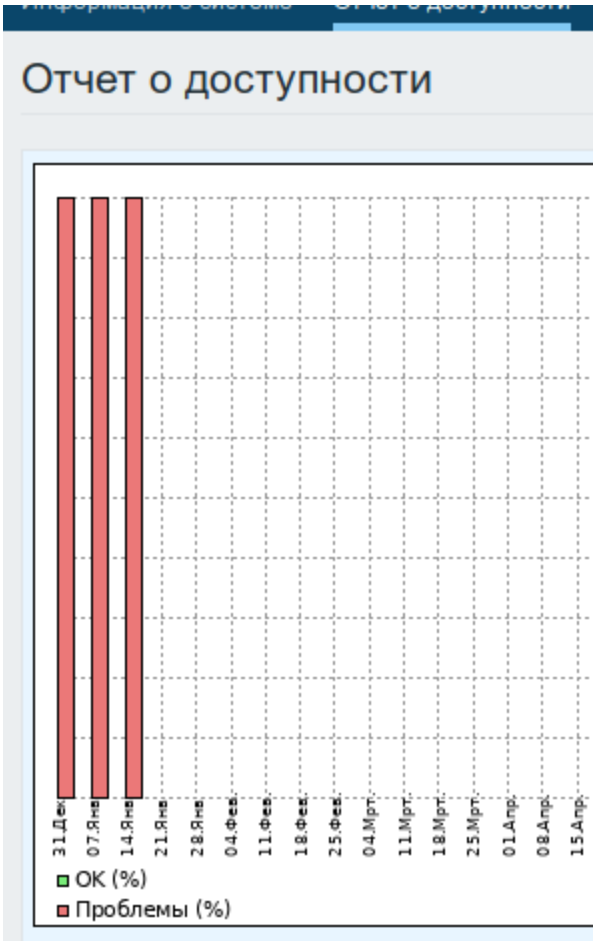


Рис. 20 График доступности

Таким образом можно проанализировать информацию и вовремя принять меры, например, заменив оборудование.

Следует отметить, что внедрение системы является экономически выгодным, так как данное ПО бесплатно и не требует лицензии. Трудозатраты на его обслуживание со стороны персонала минимальны, также снизилась загруженность персонала — меньше времени уходит на обнаружение места сбоя.

Выводы по главе 3

В данной главе были произведены следующие мероприятия:

1. Определен круг задач и мероприятий для совершенствования системы информационной безопасности колледжа
2. Проанализированы системы мониторинга корпоративных сетей
3. Выбрана система мониторинга, отвечающая заявленным требованиям
4. Система внедрена и настроена
5. Произведена оценка эффективности мероприятий

ЗАКЛЮЧЕНИЕ

На основании изученных информационных источников по теме данного исследования был сделан вывод о необходимости совершенствования системы информационной безопасности в корпоративной сети колледжа.

Вопрос об обеспечении безопасности сетей в образовательных организациях на сегодняшний день стоит очень остро ввиду повсеместной информатизации. С каждым годом в корпоративных сетях циркулирует все больше информации, сами сети расширяются и приобретают глобальный характер. Поэтому мониторинг сетей сотрудниками IT-одела — все более сложная задача.

Незаменимым помощником в данной ситуации становятся системы автоматического мониторинга сети, их актуальность и востребованность растет. В ходе данного исследования были проанализированы системы мониторинга сетей и выбрана самая оптимальная для решения поставленных задач — система мониторинга zabbix.

После внедрения и апробации системы в рабочем режиме был получен мощный инструмент, позволяющий в режиме реального времени получать информацию о состоянии сети, а так же накапливать ее для анализа и сбора статистики, что также повышает уровень безопасности сети и позволяет сделать ее более отказоустойчивой.

Благодаря внедрению мониторинга сети стало возможным существенно повысить уровень информационной безопасности, а также снять излишнюю нагрузку по выявлению неисправностей с персонала.

Таким образом, цель исследования достигнута, задачи решены, гипотеза исследования подтвердилась.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Галатенко, В.А. Основы информационной безопасности [Текст] / В. А. Галатенко. - М.: Интуит, 2013.

2. Аверченков, В. И. Организационная защита информации [Текст]: учеб. пособие / В. И. Аверченков, М. Ю. Рытов. – Брянск: БГТУ, 2014. – 184 с.

3. Автоматизированные информационные технологии в экономике [Текст]/ Под ред. И.Т. Трубилина. - М. Финансы и статистика, 2013.

4. Ясенев В.Н. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие./Ясенев В.Н. - Нижний Новгород: 2017. –198с

5. Ажмухамедов, И.М., Ханжина, Т.Б. Определение оптимального набора мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // «Актуальные вопросы современной информатики»: материалы Международной заочной научно-практической конференции (1-15 апреля 2011г.). Коломна, ГОУ ВПО «Московский гос. областной социально-гуманитарный институт», 2011, Т.1, С.8-12.

6. Ажмухамедов, И.М., Ханжина, Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности [Текст] / И.М. Ажмухамедов, Т.Б. Ханжина // Вестник АГТУ. Серия: «Экономика» №1/2011, С.185-190.

7. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 9 с.

8. ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. – Введ. 2006-12-27. – М.: Изд-во стандартов, 2006. – 7 с.

9. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.

10. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

11. Доктрина информационной безопасности Российской Федерации, № Пр-1895 от 9 сентября 2000 г.

12. Домарев, В.В. Безопасность информационных технологий. Системный подход [Текст] / В.В. Домарев. – Киев: «ТИД», 2012. – 912 с.

13. Официальный сайт ГБПОУ «Южно-Уральский государственный колледж». –URL: www.ecol.edu.ru.

14. Завгородний, В.И. Комплексная защита информации в компьютерных системах[Текст] / В.И. Завгородний. - М.: «Логос», 2001.

15. Зегжда, Д.П. Основы безопасности информационных систем[Текст]: учеб. пособие для вузов / Д. П. Зегжда, А. М. Ивашко. - М.: Горячая линия Телеком, 2000. - 452 с.

16. Концепция обеспечения информационной безопасности предприятия [Электронный ресурс]. - Режим доступа: www.securitypolicy.ru. Дата обращения: 12.05.2017.

17. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке информационных системах персональных данных с использованием средств автоматизации [Электронный ресурс]: [Утверждены руководством 8 центра ФСБ России 21.02.2008 г. №149/54-144]. - Режим доступа: www.consultant.ru. Дата обращения: 15.04.2017.

18. О безопасности [Электронный ресурс]: [федеральный закон: от 05.03.1992 г. № 2446-I, в ред. от 25.12.1992 г. № 4235-I, от 24.12.1993 г. №2288, от 25.07.2002 г. № 116-ФЗ, от 07.03.2005 г. № 15-ФЗ]. - Режим доступа: www.consultant.ru.

19. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru.

20. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г.

№149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. - Режим доступа: www.consultant.ru.

21. Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [п. 2 Постановления Правительства Российской Федерации: от 17.11.2007 г. № 781, в ред. От 01.11.2012 г. № 1119]. - Режим доступа: www.consultant.ru.

22. Петренко, С.А., Симонов, С.В., Кислов, Р.И. Информационная безопасность: экономические аспект [Текст] / С.А. Петренко, С.В. Симонов, Р.И. Кислов. – URL: http://citforum.ru/security/articles/sec/index.shtml.

23. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002.

24. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право.- Спб.: Изд-во «Юридический центр Пресс», 2001.

25. Сидоров, А.О. Модель и метод структурированной оценки риска при анализе информационной безопасности [Текст]: диссертация ... кандидата технических наук: 05.13.19 / А.О. Сидоров; [Место защиты: С.-Петерб. гос. ун-т информац. технологий, механики и оптики]. - Санкт-Петербург, 2008. - 134 с.: ил. РГБ ОД, 61 09-5/1295.

26. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004.

27. Блэк У. Интернет: протоколы безопасности. Учебный курс. - СПб.: Питер, 2001.

28. Структура системы защиты информации от угроз нарушения целостности [Электронный ресурс]. - URL: www.shadanis.narod.ru.

29. Шестерин, А.А. Совершенствование системы обеспечения информационной безопасности как составляющей экономической безопасности кредитных организаций[Текст]: диссертация ... кандидата экономических наук: 08.00.05 / А.А. Шестерин; [Место защиты: Моск. акад. экономики и права]. - Москва, 2010. - 153 с.: ил. РГБ ОД, 61 10-8/2454.

30. Бождай А.С., Финогеев А.Г. Сетевые технологии. Часть 1: Учебное пособие. Пенза: Изд-во ПГУ, 2005.

31. Владимир Шаньгин. “Защита компьютерной информации. Эффективные методы и средства”, «ДМК Пресс» 2010.

32. Симонович С., Евсеев Г. Эффективная работа: познай свой компьютер. – СПб.: Питер, 2005.

33. Свободная энциклопедия Википедия [Электронный ресурс]. – 2010. – Режим доступа: http://ru.wikipedia.org. – Дата доступа: 27.12.18

34. Указ Президента Российской Федерации от 17.12.97 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции указа Президента Российской Федерации от 10.01.2000 г. №24.

35. Шубинский М.И. Информационная безопасность для работников бюджетной сферы. Учебное пособие / НИУ ИТМО. СПб., 2012.

36. Павел Хорев. Программно – аппаратная защита информации. Учебное пособие, «Форум», 2009.

37. Основы компьютерных сетей.: Б.Д. Виснадул. – М.: Издательский дом "Форум", 2007. – 272с.

38. Кенин А.М. Самоучитель системного администратора. СПб.: БХВ-Петербург, 2012.

39. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.:ил.

40. Краковский Ю.М. Информационная безопасность и защита информации: Уч. пособие, изд-во Март, 2008

41. Казанцев С.Я., Згадзай О.Э., Оболенский Р.М. и др. Правовое обеспече-ние информационной безопасности: Учебное пособие для студентов высш. учеб. заведений. - М.: Издательский центр «Академия», 2005.

42. Акупень Т. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. №4

43. Закон Российской Федерации «О государственной тайне» от 21.07.93 №5485-1.

44. Закон Российской Федерации «О международном информационном обмене» от 04.07.96 №85-ФЗ.

45. Закон Российской Федерации «О персональных данных» от 27.07.2006г. № 152-ФЗ.

46. Дорофеев А.В. «Менеджмент информационной безопасности» Журнал «Вопросы кибербезопасности выпуск» № 3 (4) / 2014Пилипенко В. Ф., Ерков Н. В., Парфенов А. А. Обеспечение комплексной безопасности в образовательном учреждении. Теория и практика /М.: Из-во «Айрис-пресс», 2006. 192 с.

47. Гультяев А.К. Восстановление данных. – СПб.: Питер, 2005.

48. Д.П. Зегжда, А.М. Ивашко. Основы безопасности информационных сис-тем. М., Горячая линия-Телеком, 2005.

49. В.Н. Лопатин. Правовые основы информационной безопасности. Курс лекций. М., МИФИ, 2000.

50. Владимир Шаньгин. “Защита компьютерной информации. Эффективные методы и средства”, «ДМК Пресс» 2010.

51. Биячуев Т.А. Безопасность корпоративных сетей. Учебное пособие / под ред. Л.Г.Осовецкого - СПб.: СПбГУ ИТМО, 2004.

52. Блэк У. Интернет: протоколы безопасности. Учебный курс. - СПб.: Питер, 2001.

53. Бождай А.С., Финогеев А.Г. Сетевые технологии. Часть 1: Учебное пособие. Пенза: Изд-во ПГУ, 2005.

54. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом "Вильямс", 2002.

55. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право.- Спб.: Изд-во «Юридический центр Пресс», 2001.

56. Белов Е.Б., Лось В.П. Основы информационной безопасности. Учебное пособие для вузов, Гелиос АРВ, 2006.

57. «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9.09.2000 г. № Пр.-1895.

58. А. Бабаш, Е. Баранова, Д. Ларин «Информационная безопасность. История защиты информации в России», СПб.: Питер, 2015

59. А.А. Внуков ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ИНФОРМАЦИИ 2-е изд., испр. и доп. Учебное пособие для СПО. - Гриф УМО СПО, 2019.

60. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru.

ПРИЛОЖЕНИЕ

ПРИЛОЖЕНИЕ А

Инструкция по эксплуатации системы мониторинга корпоративной сети

В ходе внедрения системы мониторинга были настроены оповещения о неполадках в сети. Оповещения приходят на электронную почту персоналу технического отдела с 17:00 по 08:00 то есть в не рабочее время.

Персоналу отдела были выданы учетные данные для входа в систему. Чтобы войти в систему необходимо на стартовой странице системы ввести логин и пароль

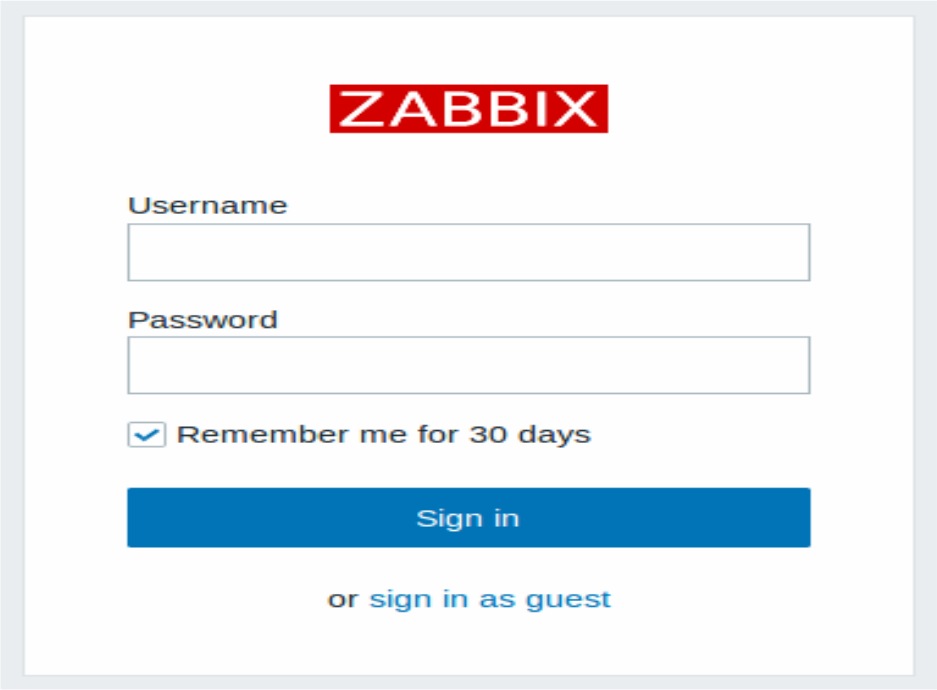


Рис. 1 Окно входа в систему мониторинга

После входа в систему открывается главный экран системы мониторинга. Он показывает основные параметры состояния системы мониторинга, а также состояния сети.

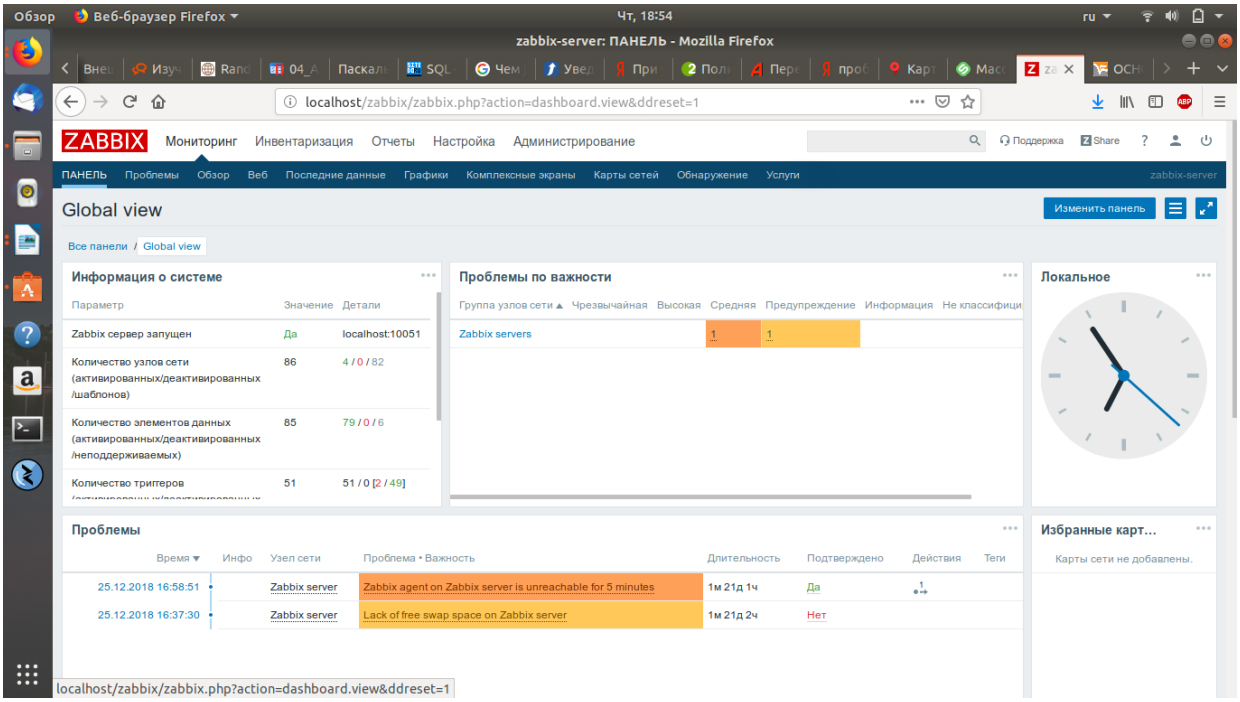


Рис. 2 Стартовый монитор системы

Если произошла неполадка в сети в разделе проблемы появится запись об этом. Она будет мигать красным. Щелкнув мышью по этой строке, можно увидеть подробности: время возникновения и сообщение о том, удалось ли устранить проблему автоматически.

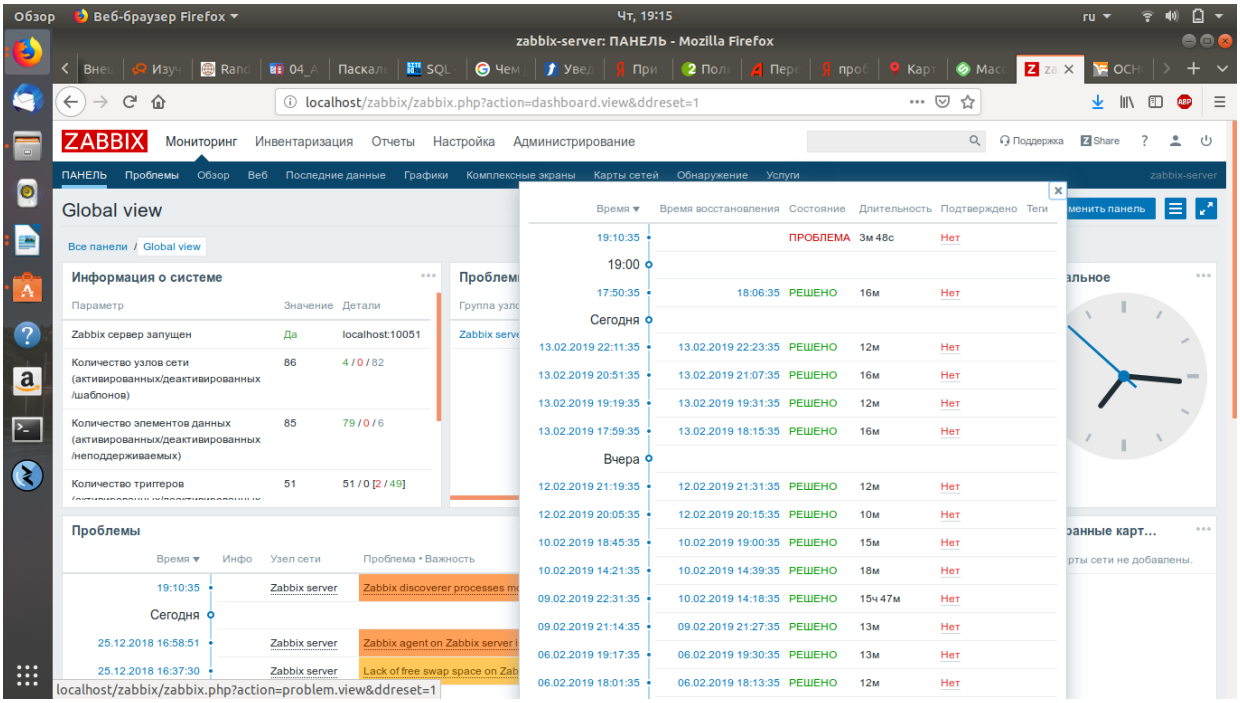


Рис. 3 Информация о проблеме

Для более детального мониторинга можно обратиться к картам сети: Меню Мониторинг — карты сети.

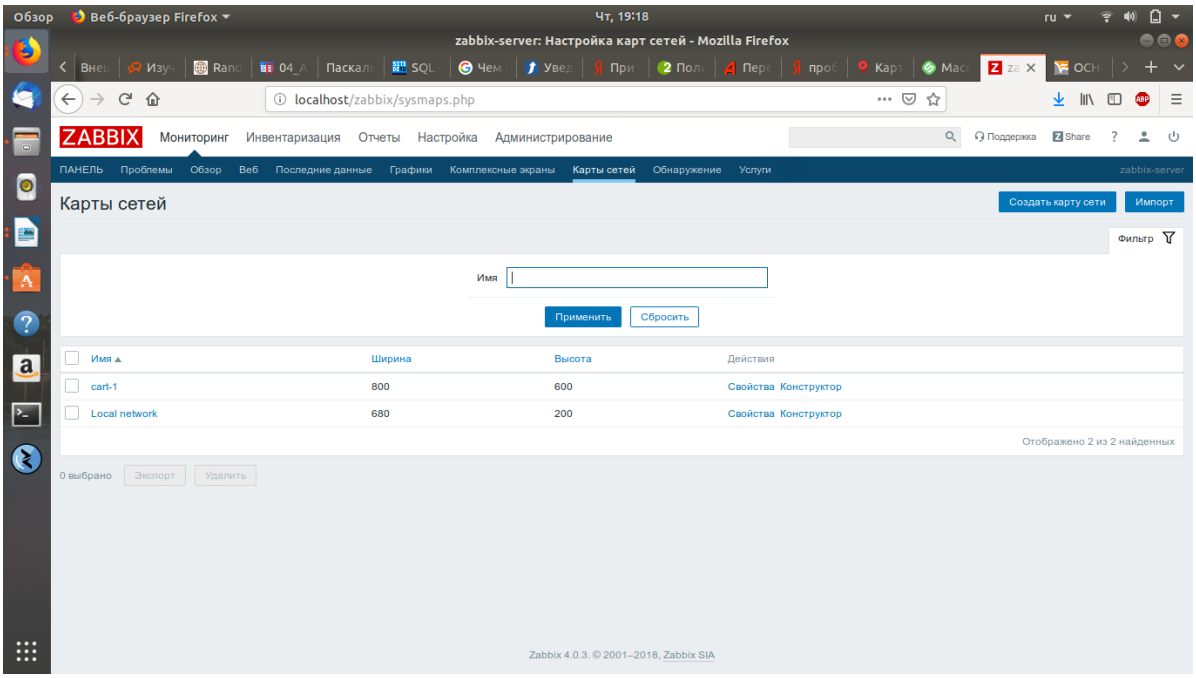


Рис. 4 Карты сети

Так же есть возможность открыть карту и наглядно посмотреть с каким узлом сети возникли проблемы.

Еще одним средством мониторинга является комплексный экран. Его можно настроить в соответствии с зоной ответственности каждого из сотрудников: Меню Мониторинг — Комплексные экраны.

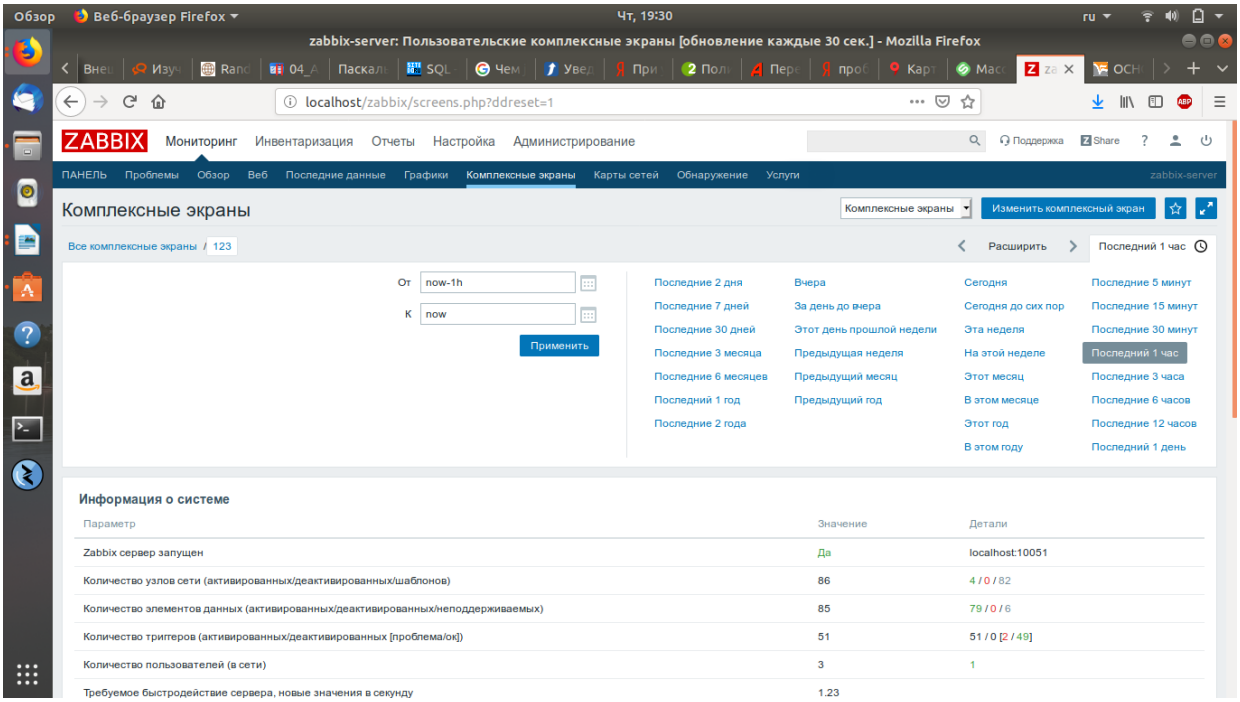


Рис. 5 Комплексный экран

Нажимаем кнопку «Изменить комплексный экран». В открывшемся окне нажимаем «+» и выбираем узел сети, а также способ его отображения

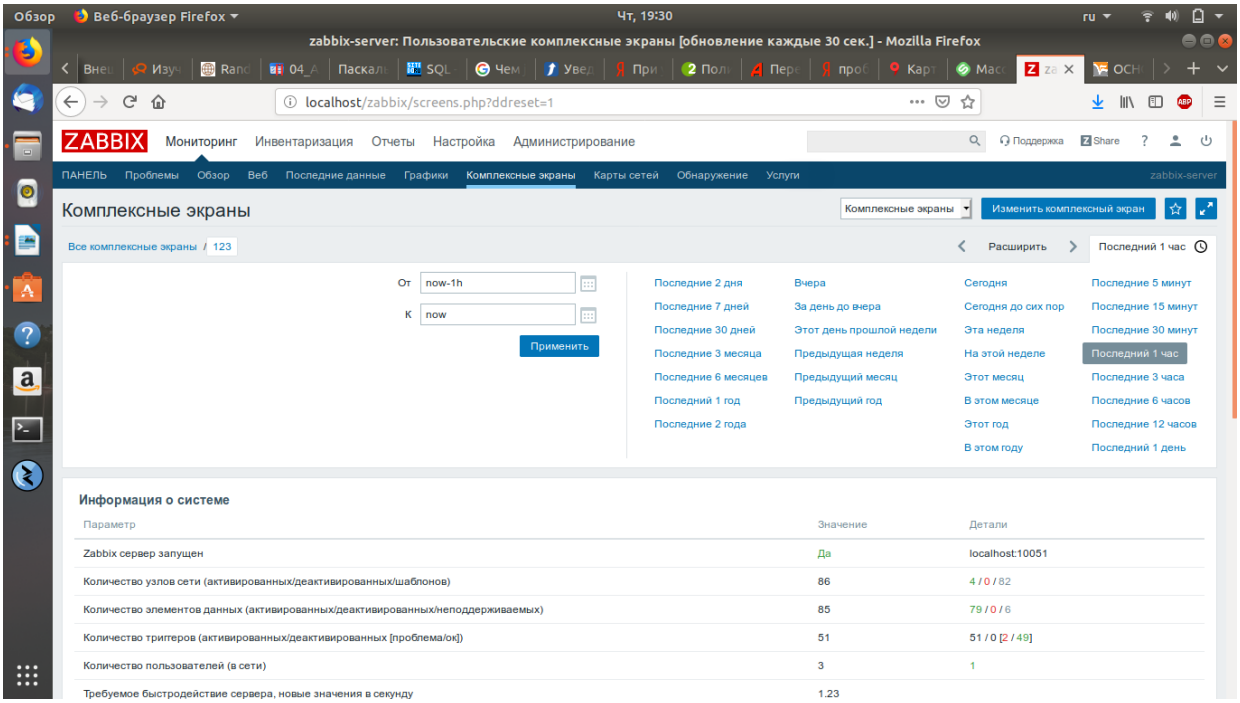


Рис. 6 Настройка комплексного экрана

В один момент времени на комплексном экране может отображаться до десяти различных параметров.

Система мониторинга позволяет собирать статистику о неисправностях в сети. Для этого существует ряд аналитических отчетов.

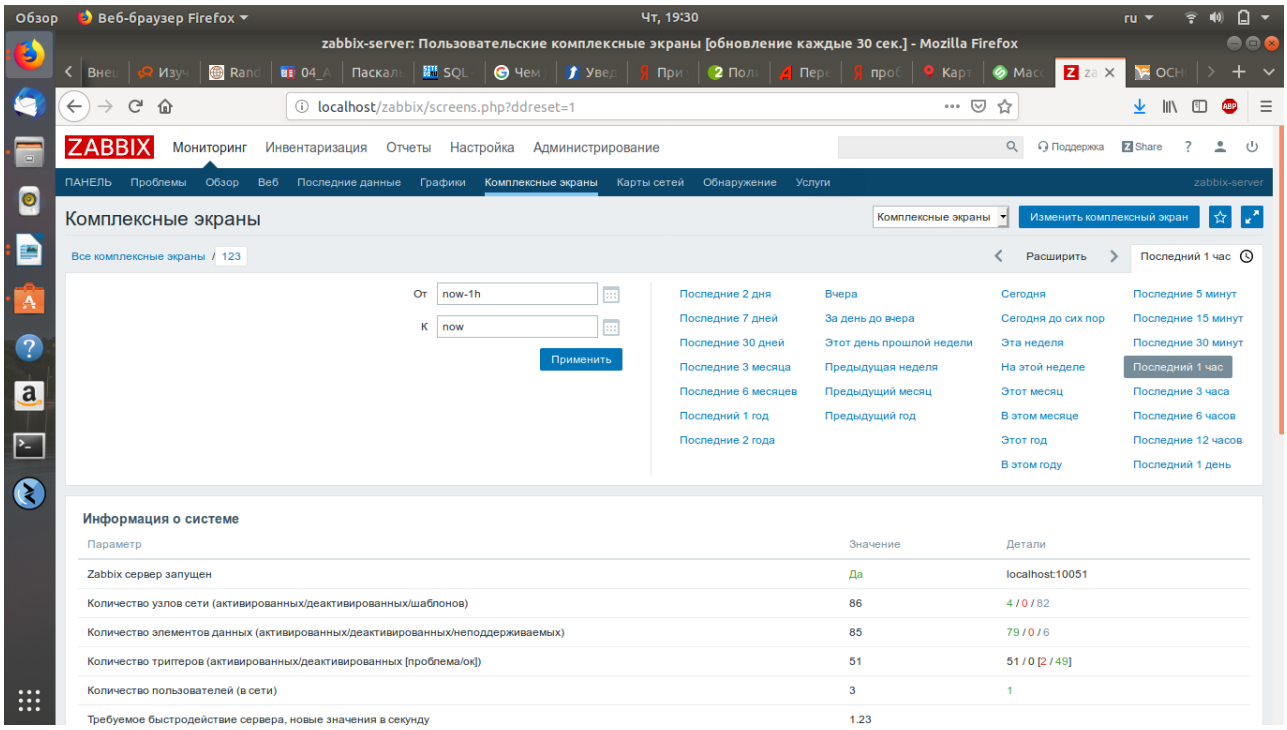


Рис. 7 Меню «Отчеты»

Отчет о доступности позволяет получить данные о неполадках во всех узлах сети за нужный отрезок времени

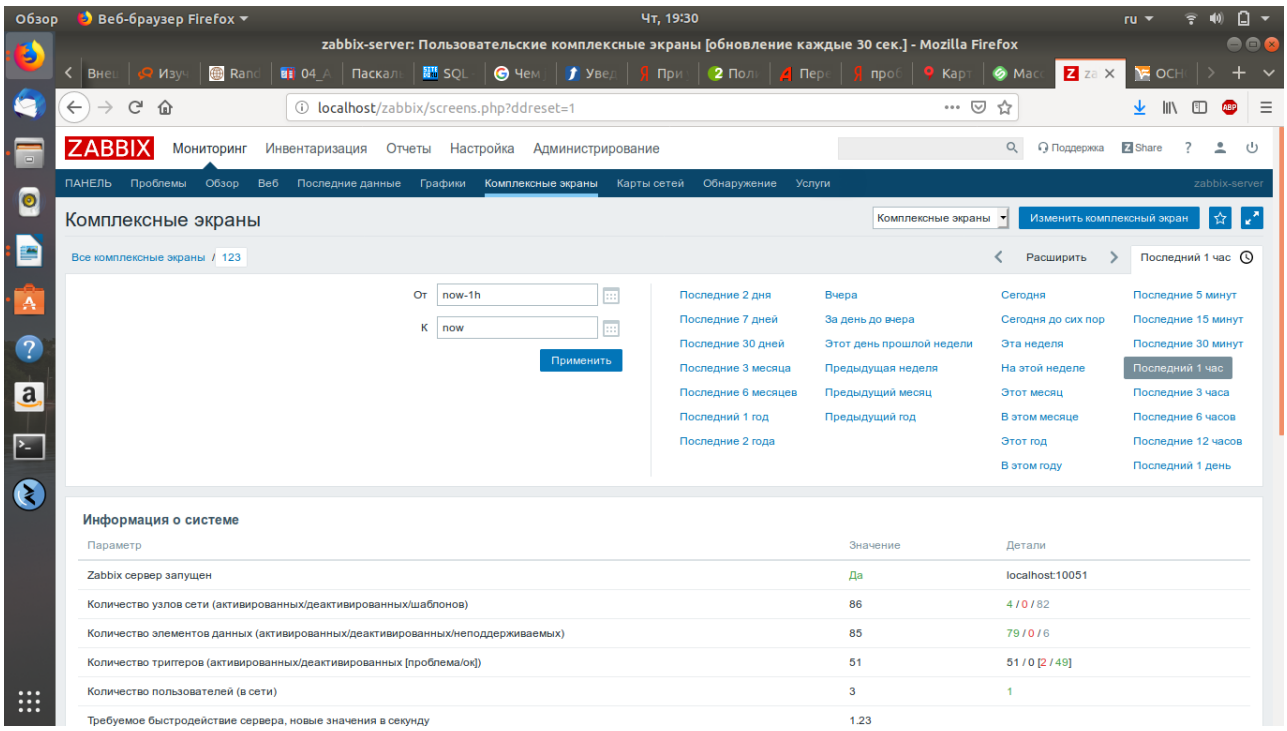


Рис. 8 Отчет о доступности

Отчет 100 наиболее активных триггеров позволяет отследить какие ошибки и неполадки возникают наиболее часто.

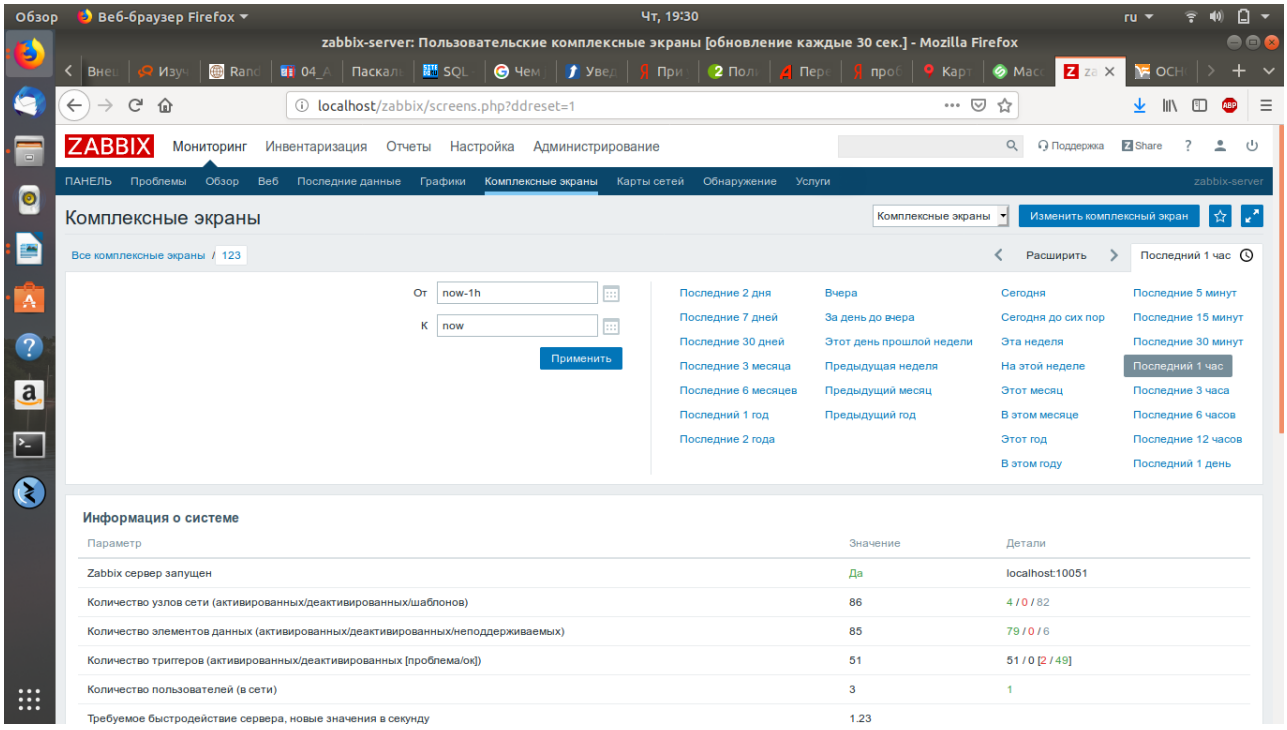


Рис. 9 100 наиболее активных триггеров