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

Выбор средств защиты корпоративной информационной системы 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:
84,59 % авторского текста

Работа рекомендована к защите
«13» 01 2025 г.
Зав. кафедрой АТИТ и МОТД
_____ Руднев В.В.

Выполнил:
Студент группы ЗФ-309-210-2-1
Гаврилюк Елена Петровна

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

Челябинск
2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном мире информационная безопасность особо актуальна, каждый год количество информации возрастает, так же как и спрос на нее, появляются новые программы для взлома информации, от рук злоумышленников страдает все больше и больше организаций. Следовательно, необходимо тщательно продумывать средства защиты от такого вида атак.

Кроме утечки обычной информации, которая может негативно отразиться на организации, большую роль играет конфиденциальная информация, которая попав не в те руки, может вызвать материальные потери. Что бы обеспечить полную защиту важной информации необходимо проделать большую работу, а именно провести полный анализ каналов утечки и выявить методы несанкционированного воздействия на информацию.

В понятие информационной безопасности образовательного учреждения 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 образовательного учреждения, можно выделить три группы:

- персональные сведения, касающиеся учащихся 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.

Ключевую роль в массовом развитии компьютерных технологий и программного обеспечения сыграли высшие учреждения. Благодаря им передовые проекты в сфере IT разрабатываются, испытываются, внедряются. С ростом онлайн преступности защита конфиденциальной информации и разработок в учебных учреждениях становится особенно актуальной.

Информационная безопасность (на уровне учреждений 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 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.

На сегодняшний день существует широкий круг систем хранения и обработки информации, где в процессе их проектирования фактор информационной безопасности хранения информации имеет особое значение. Однако, 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. Также отсутствуют труды, посвященные организации системы информационной безопасности в муниципальных и образовательных учреждениях, которые отличаются своими особенностями. Все это и обусловило актуальность темы диссертации.

В ходе изучения теоретической базы было выявлено противоречие между большим количеством материалов по информационной безопасности и ее организации в учреждении, накопленному практическому опыту в данной сфере и отсутствием актуальной информации по системам информационной безопасности в современных образовательных учреждениях. В связи с этим, определена проблема недостатка систематизации теоретических и практических материалов в контексте особенностей деятельности современных образовательных учреждений.

Цель исследования: разработать рекомендации по выбору средств защиты корпоративной информационной системы образовательной организации СПО.

Объект исследования – информационная безопасность образовательного учреждения и ее составляющие.

Предмет исследования – средства защиты корпоративной информационной системы образовательной организации СПО.

Задачи исследования:

1. Изучить и проанализировать теоретические основания для выбора средств защиты корпоративной информационной системы образовательной организации
2. Описать и проанализировать состояние информационной безопасности образовательной организации СПО, на базе учреждения «Костанайский социально-технический колледж», республика Казахстан.
3. Разработать рекомендации по выбору средств защиты корпоративной информационной системы образовательной организации - учреждения «Костанайский социально-технический колледж», республика Казахстан.

Гипотеза исследования: состояние информационной безопасности корпоративной информационной системы организации СПО повысится в случае реализации разработанных рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации СПО.

Методы исследования: изучение и анализ литературы, наблюдение.

Теоретическая и информационная база исследования представлена нормативно-правовыми актами по защите информации, внутренней документацией учреждения «Костанайский социально-технический колледж», разработки в области обеспечения информационной безопасности,

аналитические и статистические материалы по информационной безопасности.

Научная новизна исследования заключается в глубоком изучении вопросов информационной безопасности и этапов ее тестирования, поиска слабых мест, практическом тестировании информационной системы безопасности образовательного учреждения, определении особенностей работы и защиты информации и разработке рекомендаций по совершенствованию регламента работы с локальными сетями, базой данных, администрированием.

Практическая значимость работы заключается в возможности использования разработанных рекомендаций по совершенствованию, а также этапов тестирования слабых мест информационной безопасности в работе профессиональных образовательных учреждений и организаций с аналогичной спецификой работы.

Работа имеет традиционную структуру и включает в себя введение, основную часть, состоящую из 3 глав, заключение и список литературы.

Во введении обоснована актуальность выбора темы, поставлена цель и задачи анализа, охарактеризованы методы исследования и источники информации.

В первой главе раскрываются общие вопросы, исторические аспекты проблемы защиты информации. Определяются основные понятия, обуславливается актуальность звучания вопросов анализа степени защиты информационной системы колледжа.

Во второй главе рассмотрена структура учреждения, используемые меры безопасности и предосторожности, описано текущее состояние защищенности корпоративной информационной системы учреждения.

В третьей главе показаны основания и этапы разработки рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации СПО.

В заключении делаются выводы о проделанной работе согласно поставленных задач исследования.

Апробация исследования производилась путем представления докладов на научно-практических конференциях:

1. Международно научно-практическая конференции «Индустриальное развитие: технологии для людей и услуги в эпоху инноваций» 2024.
2. III Межрегиональной научно-методической конференции, г. Челябинск 21 ноября – 2024 г.
3. II Межрегиональной научно-методической конференции «Инновации в методике преподавания технических дисциплин» - 22 ноября 2023

А также путем публикации отдельных этапов исследования в научных сборниках:

1. МАТЕРИАЛЫ Международной научно-практической конференции «Индустриальное развитие: технологии для людей и услуги в эпоху инноваций», 4-5 декабря 2023 г. Тема: «Разработка и внедрение мер обеспечения информационной безопасности».
2. ВЕСТНИК НАУКИ Костанайского социально-технического университета имени академика Зулхарнай Алдамжар декабрь 2024 Тема: «Основные угрозы информационной безопасности в образование».
3. МАТЕРИАЛЫ Международной научно-практической конференции «Индустриальное развитие: технологии для людей и услуги в эпоху инноваций», 4-5 декабря 2024 г. Тема: «Информационная безопасность в деловой сфере»

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВАНИЯ ДЛЯ ВЫБОРА СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ АНАЛИЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Принципы информационной безопасности

Информация – это сведения о лицах, предметах, прецедентах, событиях, явлениях и процессах независимо от формы их представления. Информация убавляет степень неопределенности, неполноту познаний о лицах, предметах, событиях и т.д.

Защита информации – это процесс осуществления и применения в автоматизированных системах Специализированных приспособлений, поддерживающих установленный статус ее безопасности [1, с.17].

В данное время повальной компьютеризации жизнь почти всех людей находятся в зависимости от обеспечения информационной безопасности тысячи компьютерных систем обработки информации, и еще контроля и управления всевозможными объектами. К этим объектам (их именуют критическими) вполне возможно отнести системы телекоммуникаций, банковские системы, атомные станции, системы управления невесомым и наземным автотранспортом, а кроме того, системы обработки и хранения скрытой и конфиденциальной информации.

«Конфиденциальная информация – это субъективно - определяемая черта или свойство информации, указывающая на потребность введения ограничений на круг субъектов, имеющих доступ к этой информации, и обеспечения возможностью системы хранить указанную информацию втайне от субъектов, не имеющих возможностей доступа к ней. Конфиденциальная информация, которая может представлять энтузиазм для соперников обязана быть защищена» [5, с.220]. Сокрытие информации мотивируется не лишь перед ужасом утечки конфиденциальных этих, но и поползновения внести перемены в информационной базы или же рабочую документацию, что может привести не лишь к убыткам, но и затормозить работу компании. Для

обычного и не опасного функционирования систем нужно поддерживать их безопасность и целостность.

На нынешний день сформулировано три базисных принцип информационной безопасности, которая обязана обеспечить:

– целостность этих - защиту от сбоев, основных к утрате информации, и еще неавторизованного творения или же ликвидирования данных;

– конфиденциальность информации;

– доступность для всех авторизованных пользователей [7, с. 190].

– Компьютеры, часто объеденные в сеть, имеют все шансы давать доступ к грандиозному числу самых многообразных этих. Обширное становление компьютерных сети, интеграция их с информационными системами единого использования кроме положительных сторон порождает новейшие опасности безопасности информации.

Причины зарождения новых опасностей характеризуются:

– сложностью и разновидностью, применяемого программного и аппаратного обеспечения сетей;

– большим количеством узлов сети, участвующих в электронном обмене информацией, их территориальной расположенностью и отсутствием возможности контроля всех настроек;

– доступностью информации систем наружным пользователям (клиентам, партнерам и пр.) из–за ее месторасположения на физически соединенных носителях [21, с.67].

Вследствие этого люди волнуются о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением во много раз наибольшего доступа к конфиденциальным, индивидуальным или иным критическим этим.

Электронные средства хранения, в том числе и более уязвимы, чем бумажные: помещенные на них вполне возможно и уничтожить, и скопировать, и незначительно видоизменить.

Количество компьютерных правонарушений увеличивается – кроме прочего повышаются масштабы компьютерных злоупотреблений. По оценке экспертов, урон от компьютерных правонарушений растет на 35 процентов в год. Одной из обстоятельств, считается сумма наличных средств, приобретенная вследствие преступления: в тогда время как вред от среднего компьютерного правонарушения составляет 560 тысяч долларов, при ограблении банка – не более чем 19 тысяч долларов. По этим Миннесотского университета, 93 процента фирм, лишившихся доступа к своему имени на срок более 10 дней покинули собственный бизнес, кроме того половина из них сказала о собственной несостоятельности безотлагательно.

Количество служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, многократно растет. Доступ к информации больше не ограничивается исключительно тесным кругом лиц из верхнего начальства организации. Чем больше людей получают доступ к информационной технологии и компьютерному оборудованию, тем больше встает вероятностей для совершения компьютерных преступлений.

Компьютерным хакером быть может каждый. И юный взломщик и сотрудник. Компьютерные правонарушения, безупречные служащими, считают 70 – 80 процентов имеющего место быть каждый год убытка, связанного с компьютерами.

Распознание компьютерных правонарушений:

1. Неавторизованное внедрение компьютерного времени.
2. Неавторизованные поползновения доступа к файлам данных.
3. Кражи частей компьютеров.
4. Кражи программ.
5. Физическое разрушение оборудования.
6. Уничтожение этих или программ [36, с.17].

Это лишь самые явные показатели, на что принадлежит направить свой взгляд при выявлении компьютерных правонарушений. От случая к случаю

данные Распознание заявляют о том, что правонарушение уже совершено, или что не производятся меры защиты. Они кроме прочего говорят о наличии уязвимых мест, и показывают, где находится брешь в защите.

«Под информационной сохранностью понимается безопасность информации и поддерживающей ее инфраструктуры от всех нечаянных или злонамеренных действий, эффектом которых может явиться нанесение убытка самой информации, ее обладателям или поддерживающей инфраструктуре. Задачи информационной безопасности сводятся к минимизации убытка, и еще к прогнозированию и предотвращению этих воздействий» [17, с.100].

Воздействия, что наносят урон информационной безопасности организации вполне возможно поделить на несколько категорий:

1. Действия, осуществляемые авторизованными пользователями.

1) целенаправленная кража устранение этих на рабочей станции или же сервере;

2) повреждение этих пользователем вследствие беспечных действий.

2. «Электронные» способы действия, осуществляемые хакерами.

1) несанкционированное вторжение в компьютерные сети;

2) DOS-атаки.

Целью несанкционированного проникания снаружи в сеть компании быть может нанесение ущерба (уничтожение данных), кража конфиденциальной информации и внедрение ее в преступных целях, внедрение сетевой инфраструктуры для организации атак на узлы компаний, кража средств со счетов и т.п. Атака вида DOS (сокр. от Denial of Service – «отказ в обслуживании») – это наружная атака на узлы сети фирмы, соответствующие за ее не опасную и эффективную работу (файловые, почтовые сервера). Злоумышленники организуют массовую отправку пакетов этих на данные узлы, чтоб вызвать их перегрузку и, в результате, на какое – тогда время вывести их из строя. Это, как правило, влечет за собой

нарушения в бизнес процессах фирмы – потерпевшие, утрату посетителей, вред репутации и т.п.

3. Компьютерные вирусы – это разновидность вредных программ, характерной спецификой которых считается способность к размножению, повреждению или вполне истреблению.

Отдельная группа электронных способов действия – компьютерные вирусы и другие вредные программы. Они предполагают собой настоящую опасность для передового бизнеса, обширно использующего компьютерные сети, интернет и электронную почту. Вторжение вируса на узлы корпоративной сети может привести к нарушению их функционирования, утратам рабочего времени, утрата этих, краже конфиденциальной информации, причем даже прямым хищением денежных средств. Вирусная программа, проникшая в корпоративную сеть, может дать злоумышленникам выборочный или полный контроль над работой компании.

4. Спам (англ. spam) – письма, массово рассылаемые людям, не давшим согласие на их получение (относится к электронным письмам).

1) электронная почта в последнее время стала основным каналом распространения вредных программ;

2) спам отбирает массу времени на просмотр и следующее удаление сообщений, вызывает у работников чувство эмоционального дискомфорта;

3) как частные лица, так и организации становятся потерпевшими мошеннических схем, реализуемых спамерами (зачастую аналогичного семейства действия жертвы стараются не разглашать);

4) вместе с мусором часто удаляется информация, что может привести к потере посетителей, срыву договоров и прочим малоприятным результатам, опасность издержки корреспонденции особо увеличивается при применении темных списков RBL и прочих «грубых» способов фильтрации спама.

5. «Естественные» угрозы.

На информационную безопасность фирмы имеют все шансы влиять многообразные наружные факторы: предпосылкой потери этих данных готов

стать ошибочное хранение, кража компьютеров и носителей, форс – мажорные происшествия и т.д [23, с.445].

Процесс информатизации сообщества вместе с полезными результатами имеет и ряд отрицательных сторон. Каждый год увеличивается число правонарушений, в каких объектом беззаконных посягательств, считается информация, где информация в собственную очередь работает средством совершения правонарушений.

1.2 Современные методы и средства обеспечения защиты информации

Информация – один из более значимых продуктов работы человека или проявлений природы. Во всем мире информация как итог научно – тех. и платной работы являться очень дорогим продуктом. И чрезвычайно жалко (и материально накладно), когда она теряется или ее воруют, используя какие – или каналы утечки информации (подслушивают, подглядят).

Уровень становления и информатизации в Казахстане сейчас таков, что у нас нет частных больших скандалов, связанных с утечкой конфиденциальной информации. В тогда время как иностранные фирмы, учебные заведения и правительственные учреждения не рассказывают о информационных утратах, в казахстанских фирмах царит условный мир и покой. И дело не в том, что степень прозрачности нашего бизнеса позволяет беречь значительную часть корпоративной информации втайне от широкого населения. Казахстанская ментальность не дает возможность, по последней мере, творить системы, базирующиеся на полном доверии и «доброй воле» соотечественников. Несогласованность защиты платной информации с уверенностью встала перед казахстанскими организациями и учреждениями не так давно, сначала 90-х годов. В тогда время решение данной задачи рассматривалось, как правило, таким образом: достаточно все просто «запаролить», «зашифровать», поставить Особые пароли на компьютеры, и все трудности будут решены. Кроме того похожий расклад сохранялся очень

долгое время, защита информации почти во всех фирмах в общем сводилась к внедрению каких-либо технических правил [31, с. 164].

К реальному времени существуют следующие методы защиты информации, что обеспечивает требуемый уровень безопасности информации:

1. «Препятствие – содержится в существе на пути зарождения или же распространения дестабилизирующего фактора некого барьера, не позволяющего подходящему фактору принять небезопасные объемы. Обычными примерами препятствий считается блокировки, не позволяющие техническому приспособлению или программе выйти за критические границы; творение физических препятствий на пути злодеев и т.п.».

2. «Управление – есть определение на каждом шаге функционирования системы этих правящих действий на составляющие системы, следствием которых будет решение одной или же нескольких задач защиты информации».

3. «Маскировка (защищаемой информации) – подразумевает такие ее переустройства, вследствие которых она становится неприступной для злодеев или доступ к ней значительно затрудняется».

4. «Регламентация - как прием защиты информации содержится в исследовании и реализации групп событий, делающих такие условия обработки информации, при которых значительно затрудняется проявление и действие дестабилизирующих факторов».

5. «Принуждение – есть такой прием защиты, при котором пользователь и персонал должны исполнять правила и условия обработки под опасностью материальной, административной или же уголовной ответственности».

6. «Побуждение – есть метод защиты информации, при котором пользователь и персонал внутренние (т.е. материальными, моральными, этическими, психологическими и прочими мотивами) побуждаются к соблюдению всех инструкций обработки информации» [50, с. 289].

Перечисленные методы обеспечения защиты информации реализуются применением почти всех средств. Различают формальные и вовсе не формальные средства.

1. «Формальные – средства, что исполняют собственные функции по охране информации де-юре, т.е. без участия человека (физические и аппаратные)»

2. «Неформальные – средства, содержание которых составляет целенаправленная работа людей (организационные, законодательные и нравственно - этические)» [13, с.90].

Средства защиты информации – это совокупность инженерно – технических, электро, электронных, оптических и прочих приспособлений и устройств, устройств и технических систем, и еще других вещественных составляющих, применяемых для решения разных задач по защите информации, в том числе предупреждения утечки и обеспечениябезопасности защищаемой информации.

Средства обеспечения защиты информации в части предотвращения преднамеренных деяний в зависимости от приема реализации разделяются на группы:

1. «Технические (аппаратные) средства. Это разные по принципу прибора (механические, электромеханические, электронные и др.), что аппаратными средствами решают задачи защиты информации. Они мешают физическому вторжению или в случае если вторжение все таки свершилось, доступу к информации, в том числе при помощи ее конспирации. первая часть задачи решают замки, решетки на окошках, защитная сигнализация и др. вторая часть – это генераторы гула, сетевые фильтры, сканирующие радиоприемники и большое количество иных приспособлений, «перекрывающих» вероятные каналы утечки информации или позволяющих их выявить. Плюсы технических средств соединены с их надежностью, независимостью от субъективных моментов, высочайшей стойкостью к

модификации. Слабые стороны – малая эластичность, что касается немалые размер и масса, высокая стоимость».

2. «Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаление остаточной (рабочей) информации вида временных файлов, текстового контроля системы защиты и др. Плюсы программных средств – универсальность, упругость, надежность, простота установки, способность к модификации и развитию. Дефекты – ограниченная работоспособность сети, применение части ресурсов файл – сервера и сотрудников станций, высокая чувствительность к нечаянным или преднамеренным переменам, вероятная зависимость от типов компьютеров (их аппаратных средств)».

3. «Смешанные аппаратно – программные средства исполняют такие же функции, что аппаратные и программные средства в отдельности, и имеют промерные свойства» [9, с. 186].

4. «Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований лимитирования доступа к ней и др.) и организационно–правовых (национальные законодательства и правила работы, устанавливаемые руководством этого учреждения). Превосходства организационных средств состоят в том, что они позволяют решить большое количество разных трудностей, несложны в реализации, проворно откликаются на ненужные действия в сети, имеют не лимитированные возможности модификации и становления. Недочеты – высокая зависимость от субъективных причин, в том числе от совместной организации работы в точном подразделении».

5. «Законодательные средства нормативно – правовые акты, при помощи которых регламентируются права и доступ, и еще устанавливается обязанность всех лиц и подразделений, относящихся к функционированию системы, за несоблюдение инструкций обработки информации, следствием чего же быть может несоблюдение ее защищенности».

6. «Морально-этические средства, образовавшиеся в сообществе или этом коллективе нравственные нормы или этические правила, соблюдение которых содействует охране информации, а несоблюдение их равняется к неисполнению инструкций поведения в сообществе или коллективе» [9, с. 190].

Программные средства.

По степени распространения и доступности отличаются программные средства, другие средства используются в тех случаях, когда потребуется обеспечить вспомогательный уровень защиты информации;

– встроенные средства защиты информации;

– «специализированные программные средства защиты информации от несанкционированного доступа обладают, в общем, гораздо лучшими полномочиями и чертами, чем интегрированные средства».

«Кроме программ шифрования и криптографических систем, присутствует немало иных легкодоступных наружных средств защиты информации. Из более часто упоминаемых решений стоит отметить следующие две системы, позволяющие ограничить и контролировать информационные потоки»:

1. «Firewalls – брандмауэры (firewalls – пламенная стена). Меж локальной и сетью интернет делаются особые переходные серверы, что проверяют и фильтруют весь проходящий через них трафик сетевого транспортного уровней. Это дает возможность быстро понизить угрозу несанкционированного доступа снаружи в корпоративные сети, но не ликвидируют данную опасность всецело. Более защищенная разновидность способа – это прием маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewalls – сервера, делая локальную сеть фактически невидимой».

2. «Proxy-server (proxy – доверенность, доверенное лицо). Весь трафик сетевого - транспортного уровней между локальной и глобальной сетями закрывается всецело – маршрутизация как такая отсутствует, а общение из

локальной сети в масштабную происходят через специализированные серверы – посредники. Бесспорно, что при всем при этом обращения из сети интернет в локальную сеть становятся невидимыми в принципе. Данный способ мешает необходимой защиты против атак на более больших уровнях – к примеру, на уровень добавления (вирусы, код Java и JavaScript)» [24, с.58].

Аппаратные средства защиты.

В данный момент времени создано существенное количество аппаратных средств разного назначения, но большое распространение получают следующие:

1. Специальные регистры для хранения реквизитов защиты: паролей, идентифицирующих кодов, грифов или же уровней секретности.

2. Устройства измерения личных данных человека (голоса, отпечатков) с целью его идентификации.

3. Схемы прерывания передачи информации в полосы взаимосвязи с целью периодической выяснения адреса выдачи данных.

4. Устройства для шифрования информации (криптографические методы) [20, с.107].

1.3 Способы защиты информации в учреждении

«Защита информации считается своевременной темой в условиях информационной борьбы. Вопрос защиты информации поднимается уже с тех пор, когда люди научились письменной грамоте. Постоянно была информация, которую обязаны знать не все. Люди, владеющие такой информацией, прибегали к различным приемам ее защиты» [47, с.81].

О значимости сохранения информации в тайне знали уже в античные дни, когда с выходом в свет письменности была замечена и опасность чтения ее ненужными лицами. Существовали три главных метода защиты информации. Один из них надеялся защиту ее чисто силовыми методами: служба охраны документа – носителя информации – физическими лицами.

Второй прием получил название «стеганография» латино – греческое хитросплетение словечек, значащих в совокупы («тайнопись»). Он заключался в сокрытии самого прецедента присутствия информации. В этом случае применялись семантические чернила. При подходящем «проявлении» бумаги, текст становился заметным. Один из примеров сокрытия приведен в трудах древнегреческого историка Геродота. На голове раба, которая брилась наголо, записывалось необходимое известие. И когда волосы его достаточно отрастали, раба высылали к адресату, который опять брил его голову и считывал приобретенное известие. Третий метод защиты информации заключался в преобразовании смыслового слова в какой-то набор хаотических символов (или букв алфавита). Получатель этого донесения мог преобразовать его в это же самое разумное известие, в случае если владел ключом к его построению. Данный прием защиты информации называется криптографическим. Криптография – слово греческое и в переводе значит «тайнопись». По утверждению ряда экспертов криптография по возрасту – сверстник египетских пирамид. В документах старинных цивилизаций – Индии, Египта, Месопотамии – есть сведения о системах и приемах составления шифрованных посланий.

Ключевые понятия криптографии – шифр (от арабского «цифра»; арабы первыми стали сменять буквы на цифры с целью защиты начального текста). Скрытый символ, составляющий шифр, неприступный сторонним, называется ключом шифра. Как правило, в старинные дни применялись шифры замены и шифры перестановки. Историческим случаем шифра замены считается шифр Цезаря (1 век до н.э.), описанный историком древнего Рима Светонием. Гай Юлий Цезарь употреблял в собственной переписке шифр личного изобретения. Применительно к прогрессивному российскому языку он состоял в последующем. Выписывался алфавит: А, Б, В, Г, Д, Е,...,; далее под ним выписывался тот самый алфавит, но со сдвигом на три буквы влево:

При зашифровке буква А заменялась буквой Г, Б заменялась на Д, Б - Ей так дальше. Так, к примеру, слово «РИМ» преображалось в слово «УЛП».

Получатель известия «УЛП» отыскивал данные буквы в нижней строке и по буквам над ними вворачивали начальное слово «РИМ».

Одним из первых устройств, реализующих шифр перестановки, считается так именуемый устройство СЦИТАЛЛА. Он был придуман в старинной «варварской» Спарте в эпоху Ликурга; Рим сразу пользовался данным устройством. Для зашифровки слова применялся цилиндр заблаговременно обусловленного диаметра. На цилиндр наматывался изящный ремень из пергамента, и текст выписывался построчно по образующей цилиндра (вдоль его оси). После этого ремень сматывался и отправлялся - получателю известия. Последний наматывал его на цилиндр этого же диаметра и читал текст по оси цилиндра. В данном случае ключом этого шифра считался диаметр цилиндра и его длина, что, по существу, порождают двухстрочную запись, указанную выше [34, с.109].

В реальное время решения по защите и контролю информации будут крупнейшем направлением для вложений в ближайшие 5 лет в перспективе подъема. Количество конфликтов с утечкой данных и требований правительственных регулирующих органов, признает исследовательская фирма IDC в тематическом докладе.

«Кроме того, по мониторингам фирмы, мировой рынок защиты информации в 2021 году превзойдет размер в $ 13 млрд., раз, в год увеличиваясь на 33 %. «Информация стала новой СКВ мира, - сообщает менеджер по изысканиями IDC”s Security Product program Брайан Бурке в своем докладе – Увеличивающееся количество больших конфликтов сделало взрывной спрос на решения, защищающие от умышленной или же неумышленной утечки информации» [33].

«Меры защиты – это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных приспособлений или добавочных программ, главной целью которых считается предотвращение правонарушений и злоупотреблений. Составление

режима информационной безопасности – групповая несогласованность. Меры по ее решению вполне возможно поделить на 4 уровня» [29, с.90]:

- законодательный: законы, нормативные акты, стереотипы и т.п.;
- административный: действия совместного нрава, предпринимаемые руководством организации;
- процедурный: точные меры безопасности, имеющие дело с людьми;
- программно-технический: точные технические меры.

В данное время более доскональным законодательным документом считается Закон Республики Казахстан от 11.01.2007 №217 – III

«Об информатизации».

Рассмотрим некоторые способы защиты информационной безопасности компьютерных систем:

1. Аутентификация пользователя. Эта мера потребует, чтобы пользователи исполняли процедуры входа в компьютер, используя это как средство для идентификации сначала работы. Для аутентификации персоны каждого пользователя необходимо применять неповторимые пароли, не являющиеся комбинациями своих этих пользователей. Нужно будет ввести меры защиты при администрировании паролей, и ознакомить пользователей с погрешностями, позволяющими осуществить компьютерное правонарушение. Если в компьютере существует интегрированный шаблонный пароль, его надо непременно поменять. Еще более верное решение состоит в организации контроля доступа в помещения или к определенному компьютеру сети при помощи идентификационных пластмассовых карточек встроенной микросхемой – так именуемых микропроцессорных карточек (smart - card). Их надежность обусловлена в первую очередь невыполнимостью копирования или подделки кустарным методом. Установка специального считывающего приспособления этих карточек вероятна не лишь на входе в помещения, где находятся компьютеры, но и именно на сотрудников и серверах сети. Существуют, кроме того, разные приспособления для

идентификации персоны по биометрической информации – по радужной оболочке глаза, следам пальцев, объемам кисти руки и т.д.

2. «Защита пароля. В наше время больше обостряется хищение паролей. И, как проявляет статистика, в основном количестве случаев злоумышленнику удается похитить пароль потерпевшие только лишь вследствие пренебрежительности или же доверчивости жертв. Существуют следующие правила для защиты пароля»:

1) нельзя делиться собственным паролем ни с кем;

2) пароль обязан быть тяжело угадываемым;

3) для осуществления пароля надо применять строчные и прописные буквы, а еще гораздо лучше разрешить компьютеру лично сгенерировать пароль;

4) не рекомендовано применять пароль, который считается адресом, псевдонимом, именованием родственника, телефонным номером или чем–то очевидным;

5) предпочтительно применять длинные пароли, т.к. они более безопасны, лучше всего, чтоб пароль состоял из восьми и более символов;

6) пароль не должен отображаться на экране компьютера при его вводе;

7) пароли должны отсутствовать в распечатках;

8) нельзя записывать пароли на столе, стене или же терминале, его необходимо держать в памяти;

9) пароль необходимо время от времени поменять и делать это не по графику;

10) на должности администратора паролей обязан быть самый надежный человек;

11) не рекомендовано применять один и тот же пароль для всех работников в группе;

12) когда работник увольняется, нужно будет заменить пароль;

13) сотрудники обязаны расписывать за получение паролей [7, с.172].

3. Процедуры авторизации. В организации, имеющей дело с критическими данными, обязаны быть разработаны и внедрены процедуры авторизации, что характеризуют, кто из пользователей обязан иметь доступ к той или другой информации и приложениям. В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля потребуется разрешение тех или других начальников. Если информация обрабатывается в большом вычислительном центре, тогда нужно контролировать физический доступ к вычислительной технике. Имеют все шансы сказаться уместными такие способы, как журналы, замки пропуска, также служба охраны. Ответственный за информационную безопасность обязан знать, кто имеет право доступа в здание с компьютерным оборудованием, и выгонять от туда посторонних.

Осторожность при работе.

Рекомендуется:

1) отключать неиспользуемые терминалы;

2) закрывать комнаты, где пребывают терминалы;

3) разворачивать экраны компьютеров так, чтоб они не были заметны со стороны двери, окошек и других мест, что не контролируются;

4) установить специализированное оборудование, ограничивающее количество неуспешных попыток доступа, или делающее обратный звонок для выяснения личности пользователей, использующих телефонные аппараты для доступа к компьютеру;

5) использовать программы отключения терминала после особого периода неиспользования;

6) выключить систему в нерабочие часы;

7) использовать системы, позволяющие после входа пользователя в систему извещать ему время его заключительного сеанса и количество неуспешных попыток установления сеанса после этого. Это даст возможность сделать пользователя деталью системы ревизии журналов [25, с.17].

4. «Физическая безопасность. В защищаемых компьютерных системах нужно будет принимать конструктивные меры по предотвращению, обнаружению и минимизации убытка от пожара, наводнения, загрязнения находящейся вокруг среды, повышенных температур и скачков напряжения. Пожарная сигнализация и системы пожаротушения обязаны периодически проверяться. Компьютера вполне возможно отстоять при помощи кожухов, чтоб они не были повреждены системой пожаротушения. Горючие материалы не обязаны храниться в данных кабинетах с компьютерами». Температура в помещении может контролироваться кондиционерами и вентиляторами, и еще обычной вентиляцией в помещении. Трудности с повышенной температурой имеют все шансы появиться в стойках периферийного оборудования или вследствие закрытия вентиляционного отверстия в терминалах или компьютера, вследствие этого нужна их постоянная ревизия. Предпочтительно использование невесомых фильтров, что может помочь очистить воздух от веществ, что могут нанести урон компьютерам и дискам. Стоит запретить курить, брать с собой еду и употреблять ее около компьютера. Компьютеры обязаны располагаться как вполне возможно далее источников большого числа воды (трубопроводов).

5. «Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток)».

Для защиты носителей информации рекомендуется:

1) вести, контролировать и проводить проверку реестры носителей информации;

2) обучать пользователей правильным способам очистки и ликвидации носителей информации;

3) делать, уловки на носителях информации, отражающие уровень критичности содержащейся в них информации;

4) уничтожать носители информации согласно с проектом организации;

5) доводить все важные документы до сотрудников;

6) хранить диски в конвертах, коробках, железных сейфах;

7) осторожно вставлять диски в компьютер и держать их подальше от источников магнитного поля и солнечного света;

8) убирать диски и ленты, с которыми в реальный момент не проводится работа;

9) хранить диски разложенными по полкам в особом порядке;

10) не давать носители информации с важной информацией не тем людям;

11) выбрасывать или же отдавать покоробленные диски с важной информацией лишь после их размагничивания или же аналогичной процедуры;

12) уничтожать важную информацию на дисках при помощи их размагничивания или же физического разрушения согласно с порядком в организации;

13) уничтожать распечатки и красящие ленты от принтеров с важной информацией согласно с порядком организации;

14) обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру [46, с.192].

6. «Выбор правильного оборудования. Производительность и отказоустойчивость информационной системы во многом находится в зависимости от работоспособности серверов. При потребности обеспечения круглосуточной бесперебойной работы информационной системы употребляются некоторые отказоустойчивые компьютеры, т.е. такие, выход из строя отдельного составляющих запчастей, отказ которых приводит к отказу машины. На надежность информационных систем негативно сказываются и присутствие приспособлений, собранных из девайсов невысокого качества, и внедрение нелицензионного ПО. Излишняя бережливость средств на изучение персонала, закупу компьютеров лицензионного программного обеспечения и высококачественного оборудования приводит к уменьшению времени безотказной работы и большим расходам на следующие восстановления системы».

7. «Источники бесперебойного питания. Компьютерная система энергоемка, и потому первое условие ее функционирования – бесперебойная предоставление электричества. Достаточной долей информационной системы должны быть информаторы бесперебойного питания для серверов, а по возможности, и для всех локальных сотрудников станций. Рекомендовано кроме того дублировать электропитание, используя для этого всевозможные городские подстанции. Для кардинального решения задачи вполне возможно установить резервные силовые полосы от личного генератора организации».

8. Разработка адекватных проектов обеспечения бесперебойной работы и восстановления. Целью является: обеспечение постоянной работы и восстановления считаются гарантией того, что пользователи сумеют продолжать беспрерывно исполнять собственные, самые основные дела в случае невозможности дел сосредоточенных на информационной технологии. Обслуживающий персонал обязан знать, как им работать по данным проектам. Проекты обеспечения ошибочной работы и восстановления (ОНРВ) обязаны быть прописаны, проверены, и периодически проводиться для служащих. Процедуры намерения обязаны быть адекватны уровню безопасности и важной информации. Проект ОНРВ может применяться в условиях неразберихи и паники, вследствие этого надо постоянно проводить тренировки сотрудников.

9. «Резервное копирование. Одним из основных, эпизодов которые обеспечивают восстановление системы при потере данных, считается резервное копирование сотрудников программ и. В локальных сетях, где установлены несколько серверов, больше всего система резервного копирования устанавливается именно в свободные слоты серверов. В больших корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и сотрудников организации в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании. Для архивной

информации, представляющей специальное значение, рекомендовано учитывать охранное здание». Дубликаты более значимых копий, гораздо лучше беречь в другом здании или в том числе и в другом городе. Исключительная мера делает эти данные не уязвимыми в случае пожара или иного стихийного бедствия [39, с.192].

10. Дублирование, мультиплексирование и резервирование кабинетов. Кроме резервного копирования, которое выполняется при появлении внештатной ситуации или по заблаговременно составленному расписанию, для большей сохранности данных на жестких дисках используются специализированные технологии - зеркалирование дисков и создание RAID – массивов, что предполагают собой сообщество нескольких жестких дисков. При записи информация поровну распределяется между ними, и при выходе из строя одного из дисков оказавшиеся на нем данные имеют все шансы быть восстановлены по содержимому. Технологии кластеризации представляют, что несколько компьютеров работают как единое целое. Кластеризуют, как правило, серверы. Один из серверов кластера может работать в режиме горячего резерва с уверенностью готовности начать быстро исполнять функции главной машины в случае ее выхода из строя. Продолжением технологии кластеризации считается распределенная кластеризация, при которой через сеть интернет объединяются несколько кластерных серверов, разнесенных на большое расстояние. Распределенные кластеры близки к понятию резервных на большое расстояние. Распределенные кластеры близки к понятию резервных представительств, нацеленных на обеспечение жизнедеятельности компьютера при ликвидировании его центрального помещения. Резервные кабинеты делят на прохладные, в каких проведена коммуникационная разводка, но отсутствует какое – или оборудование и жаркие, которыми имеют все шансы быть дублирующим вычислительным центром, получившим всю информацию из центрального представительства, филиала и т.д.

11. «Резервирование каналов взаимосвязи. При неимении взаимосвязи с наружным миром и собственными подразделениями, кабинет как оказалось парализованным, потому большое значение имеет резервирование наружных и внутренних каналов взаимосвязи». «При резервировании рекомендовано соединять различные виды взаимосвязи – кабельные линии и радиоканалы, невесомую и подземную прокладку коммуникаций и т.д. По мере того, как фирмы больше и больше обращаются к Internet, их проект как оказалось в сильной зависимости от функционирования Internet – провайдера. У поставщиков доступа к сети приключаются достаточно большие трагедии, вследствие этого важно сохранять все весомые прибавления во внутренней сети фирмы и иметь договора с несколькими районными интернет - провайдерами. Необходимо кроме того заблаговременно придумать прием оповещения стратегических посетителей о изменении электронного адреса и настоятельно просить от провайдера проведения мероприятий, которые обеспечивают оперативное восстановление его услуг после аварий» [32, с.18].

12. «Защита от перехвата. Для каждых из трех главных технологий передачи информации присутствует разработка перехвата: для кабельной линий – включение к кабелю, для спутниковой взаимосвязи – внедрение антенны приема сигнала со спутника, для радиоволн – радиоперехват. Казахстанские службы безопасности разграничивают коммуникации на три класса. Первый обхватывает локальные сети, находящиеся в зоне безопасности, т.е. местности с урезанным доступом и за экранированным электронным оборудованием и коммуникационными линиями, и не имеющие выходов в каналы взаимосвязи за ее пределами». Ко второму классу относятся каналы взаимосвязи вне зоны безопасности, защищенные организационно – техническими мерами, а к третьему – беззащитные каналы взаимосвязи единого использования. Использование коммуникаций уже второго класса существенно сокращает возможность перехвата этих. Для защиты информации в наружном канале взаимосвязи употребляются следующие устройства: скремблеры для защиты речевой информации,

шифраторы для широковещательной взаимосвязи и криптографические средства, обеспечивающие шифрование цифровых этих. Главнейшими данными алгоритмов шифрования считаются крипто стойкость, длина ключа и скорость шифрования.

В данное время более часто используются три ключевых эталона шифрования:

- AES;
- «RSA – система, в какой шифрование и расшифровка осуществляется при помощи различных ключей»

За работу системы отвечает администратор сети. Системный администратор (от англ. system administrator) – работник, должностные обязанности которого обеспечение штатной работы парка компьютерной техники сети и программ в организации. Системные администраторы противостоят атакам взломщиков и позволяют безопасно связываться внутри инфраструктуры фирмы, также за ее пределами.

Многофункциональные прямые обязанности системного администратора.

На администратора сети возлагаются следующие функции:

- оперативно-техническое руководство и обеспечение бесперебойного функционирования локальной вычислительной сети;
- контроль над техническим состоянием технических средств вычислительной сети;
- выявление и исправление сбоев в работе сети;
- обеспечение взаимодействий с другими сетями передачи данных;
- методическое обеспечение надлежащих вопросов [37, с.192].

Для исполнения возложенных на него функций администратор сети исполняет следующие обязанности:

- организует и обеспечивает бесперебойное функционирование локальной вычислительной сети;

- устанавливает на серверы и рабочие станции сетевой программное обеспечение, конфигурирует систему на сервере;
- обеспечивает интегрирование программ на файл-серверах, серверах систем управления базами этих и на сотрудников;
- поддерживает рабочее состояние программного обеспечений сервера;
- обеспечивает защиту от несанкционированного доступа к информации, просмотра или же изменение системных файлов и этих, и еще безопасность межсетевого взаимодействия;
- организует доступ к локальным и масштабным сетям, в т.ч. в сеть интернет; обмен информацией с другими организациями с внедрением электронной почты [18, с.193].

1.4 Компьютерные вирусы и их классификация

«Компьютерные вирусы – это специально прописанная не очень большая по объемам программа, имеющая специфический метод, направленный на массовые копии программы, или ее модификацию и исполнению увеселительного, пугающего или разрушительного эффекта» [27, с.17].

Тем или же другим методом вирусная программа попадает в компьютер и заражает их. Программа, внутри которой пребывает вирус, называется зараженной. Когда эта программа начинает работу, тогда с начала управление получает вирус. Вирус находит и заражает иные программы, а еще исполняет какие-либо вредные действия. К примеру, меняет файлы или же таблицу размещения файлов на диске, занимает оперативную память и т.д. После того, как вирус выполнит собственные действия, он передает управление той программе, в какой он располагается, и она действует как обычно. Тем самым на вид работа зараженной программы смотрится так же, как и незараженной. Поэтому далеко не сразу пользователь выяснит о пребывании вируса в компьютере. Почти все разновидности вирусов устроены так, что при запуске

зараженной программы вирус остается в памяти и время от времени заражает программы и исполняет ненужные действия на компьютере. Пока же на компьютере заражено мало программ, присутствие вируса, может быть почти что незаметным.

К количеству более отличительных симптомов инфицирования компьютера вирусами относятся следующие:

- некоторые раньше исполнявшиеся программы перестают, запускаться или неожиданно останавливаются в ходе работы;
- увеличивается размер исполняемых файлов;
- быстро сокращается размер свободной дисковой памяти;
- на носителях возникают вспомогательные кластеры, в каких вирусы прячут собственные фрагменты или части испорченных файлов;
- замедляется работа каких-либо программ;
- в текстовых файлах бывают замечены бесполезные фрагменты;
- наблюдаются пробы записи на защищенную дискету;
- на экране возникают странные сообщения, что ранее не наблюдались;
- появляются файлы с непонятными датами и временем создания (несуществующих месяцев, годы, часы, минуты и секунды, не укладывающиеся в общепризнанные интервалы и т.д.);
- операционная система перестает загружаться с винчестера;
- появляется известия об отсутствии винчестера;
- данные на носителях портятся [48, с.123].

Один из каналов распространения вирусов, имеющий отношение к делам связанным с компьютерными сетями, считается Internet. Часто источниками инфицирования считаются программные продукты, приобретенные незаконным методом.

Присутствует несколько классификаций компьютерных вирусов:

1. По среде обитания различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.

2. По приему заражения выделяют резидентные и нерезидентные вирусы.

3. По степени действия вирусы бывают неопасные, небезопасные и чрезвычайно опасные.

4. По отличительным чертам алгоритмов вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро – вирусы [49, с.192].

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

В первой главе мы рассмотрели общие вопросы, историю и проблемы защиты информации, принципы информационной безопасности.

Также были рассмотрены современные методы и средства обеспечения защиты информации. Определили основные понятия, обуславливаемые актуальность вопросов степени защиты информационной системы колледжа.

Проанализировали основные способы защиты информации в учреждении и более детально познакомились с системой информационной безопасностью колледжа.

Изучили наиболее активные и опасные современные компьютерные вирусы, их классификацию, распространения и влияние на работу компьютеров и информационных систем учреждения, а также рассмотрели способы защиты информационной безопасности компьютерных систем колледжа.

ГЛАВА 2. СОСТОЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ «КОСТАНАЙСКИЙ СОЦИАЛЬНО - ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

2.1 Описание объекта исследования

Учреждение «Костанайский социально-технический колледж» является структурным подразделением Костанайского социально-технического университета им. академика З. Алдамжар. Основателем является Зулкарнай Алдамжар, доктор исторических наук, профессор, академик Международной академии наук высшей школы Казахстана и Международной академии информатизации, Почетный гражданин штата Техас (США) и Почетный гражданин г. Костаная. Начало образовательной деятельности – 1999г. До 2005 года носил название «Костанайский социально-экономический колледж». Директором является Шукманова Роза Сеитхановна. Учреждение имеет 2 основных корпуса: первый расположен по адресу г.Костанай, улица Тәуелсіздік, 118 «Б», второй корпус расположен по адресу проспект Кобыланды батыра 31. Телефон, факс: 8 (7142) 54-47-53. Электронный адрес: mail@kstc.edu.kz, сайт: https://kstc.edu.kz. Общая площадь составляет 13965, 5 кв.м.

В 2018 году колледж успешно прошел институциональную и специализированную аккредитацию по специальностям «Физическая культура и спорт» и «Электроснабжение (по видам)».

Колледж ведет подготовку специалистов по 11 специальностям: «Организация перевозок и управление движением на ж/д транспорте», «Вычислительная техника и программное обеспечение (по видам)», «Электроснабжение (по отраслям)», «Экология и природоохранная деятельность (по видам)», «Делопроизводство и архивоведение (по отраслям и областям применения)», «Правоведение», «Менеджмент (по отраслям и областям применения)», «Финансы (по отраслям)», «Переводческое дело»,, «Физическая культура и спорт», «Дошкольное воспитание и обучение».

Колледж делится на три отделения: Техническое, «Физическая культура и спорт», «Управление, экономика и право».

На данный момент в учреждении обучается 1026 студентов. Из них 909 по очной форме обучения, 123 по заочной форме обучения.

Всего в колледже имеется 12 компьютерных классов, 248 персональных компьютеров, которые используются в учебном процессе, имеющие доступ к сети интернет (рисунок 1).

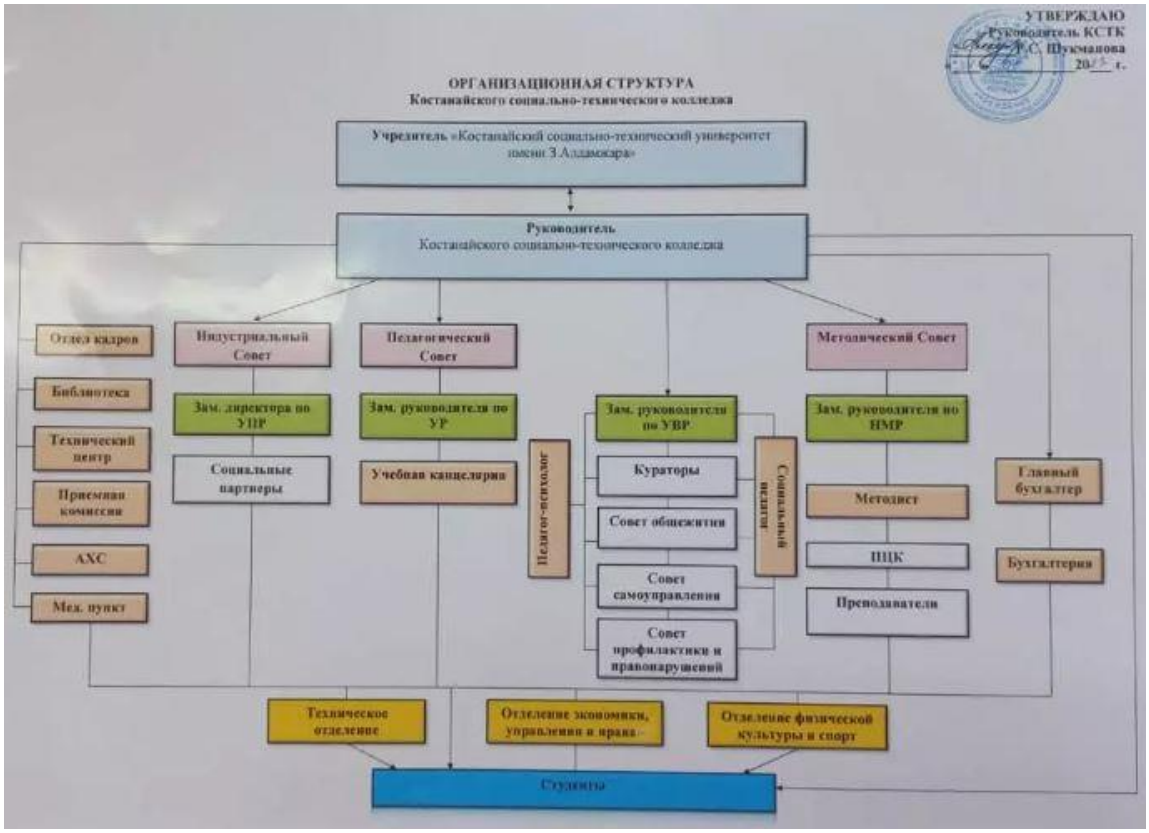

Рисунок 1 – Структура колледжа

Информационно-технический центр.

Короткая информация о подразделении: Информационно-технический центр обслуживает Учреждение «Костанайский социально-технический колледж» и Костанайский социально-технический университет им, академика З. Алдамжар (ИТЦ).

В своей деятельности ИТЦ руководствуется Уставом колледжа, университета, распоряжениями ректора университета и директора

колледжа, нормативными материалами, касающимися деятельности ИТЦ (эксплуатация и обслуживание вычислительной и копировально-множительной техники), правилами и нормами охраны труда и техники безопасности.

Задачи: поддержка учебного процесса

В состав подразделения входят: 1 – Начальник ИТЦ, 1 – Системный администратор, 2 – Инженера-программиста ИТЦ, 1 – Инженер электронщик

Короткая историческая справка:

Для целенаправленного внедрения и становления, координации информатизации в колледже был организован Информационно-технический центр (ИТЦ) в начале сентября 2004 года.

Информационно-технический центр ИТЦ считается структурной единицей КСТК, осуществляющей системное введение и становление информационно-коммуникационных технологий (ИКТ) в колледже, разработку, реализацию и сопровождение планов, формирующих единую мульти сервисную образовательную среду. Вся работа ИТЦ осуществляется сообразно концепций создания и становления мульти сервисной среды КСТК и групповых программ развития

«Основой ЕМОС считается образовательный портал Костанайского социально – технического колледжа. Мульти сервисность портала поддерживается информационным web-сайтом, АИС Platonus, сопровождающей автоматизированный документооборот в учебном процессе, сам учебный процесс по кредитной технологии, почтовым обслуживанием, файлообменником и др» [42, с.13].

На данный момент наблюдается наращивание функциональности ЕМОС за счет:

1. Развития учебных компьютерных компонентов.
2. Расширения организационно-управленческой системы.
3. Расширения научно-исследовательской системы.
4. Расширения вне учебных компьютерных компонентов.

Создана техническая инфраструктура колледжа:

1. «Корпоративная сеть, состоящая из более 200 компьютеров, на базе Fast Ethernet со скоростью передачи этих 100 Мб/с и протяженностью 10 км «витой пары» внутри 2-х учебных корпусов.

2. «Соединение между вышеуказанными корпусами осуществляется по технологии WiFi, средством использования нацеленных антенн, со скоростью передачи этих до 100 Мб/с».

3. «В каждом корпусе и на каждом этаже установлены узлы (точки доступа к серверам корпоративной сети) беспроводной взаимосвязи для ноутбуков и нетбуков студентов и сотрудников колледжа, в частности, для конференц-зала, для читальных залов».

4. «Доступ в Сеть интернет поддерживается по оптоволокну Казактелеком на скорости 60 Мбит/с и провайдер Uplink со скоростью 100 Мбит/с».

Одной из новаторских информационных технологий считается применение образовательного портала КСТК не исключительно в корпоративной сети, ведь и в глобальной сети, т.е. выход средством веб-сайта КСТК всякому студенту и работнику колледжа на сервер автоматизированной информационной системы (АИС) Platonus, полностью удовлетворяющей кредитной системы преподавания. В частности, студент, с момента зачисления и до окончания государственным экзаменом собственной образовательной линии движения, присутствует в информационной базе этой АИС, т.е. весь учебный процесс студента проходит в онлайн-режиме». В данной системе: популярность, получение, исполнение заданий учителя сообразно календарного проекта в виртуальной аудитории, переписка с учителем, со студентами, фиксация успеваемости в журнале, рубежный контроль, тестирование, выдача ведомостей и т.д..

«Для применения всех вероятностей компьютерной техники в колледже ведутся мероприятия сосредоточенные на интеграции информационно-коммуникационных технологий. Потому что КСТК каждый

день использует видеоконференцсвязь внутри колледжа для проведения дистанционных занятий. Длится введение в учебный процесс интерактивных электронных досок в мультимедийных аудиториях колледжа. Изучение казахскому, английскому языкам, проведение интерактивных занятий по химии, физике и информатике осуществляется в 20 специализированных аудиториях.

Сотрудники информационно-технического центра КСТК и учителя кафедры разработали программы подготовки, и переподготовки в сфере кадров ИТЦ придумали рабочие программы связанных с внедрения и применения информационно-коммуникационных технологий. По программе «Изучение Office: текстовый процессор Writer, табличный Calc, презентационный редактор Impress» прошли курсы для 3 групп по 20 слушателей на казахском и английском языках, а при исследовании операционной системы Microsoft Windows 10 более 50 слушателей различного уровня подготовки [25, с.10].

«Кроме того прошел семинар для работников учебного отдела, офис-регистраторов, ППС кафедр (сего более 30 слушателей) с выдачей сертификатов по применению АИС Platonus (автоматизация документооборота и учебного процесса по кредитной технологии)».

Материально-техническая база:

Компьютеров - 248, 12 компьютерных классов, интерактивные панели 30 шт., 3 D принтер – 5 шт., электронный микроскоп для проведения лекционных и лабораторных занятий, приобретены сервера, программные обеспечения, система видеонаблюдения, поддержка провайдеров доступ в Сеть интернет поддерживается по оптоволокну Казактелеком на скорости 60 Мбит/с и провайдер Uplink со скоростью 100 Мбит/с.

Для доступа Веб, для проведения Online уроков, лекций и видеоконференций приобретено оборудование Polycom.

2.2 Единая мульти сервисная образовательная среда

Единая мульти сервисная образовательная среда (ЕМОС) – это аппаратно-программный компьютерный комплекс для внедрения интерактивных технологий в процесс преподавания, включающий в себя важное оборудование, программное обеспечение с большим количеством разновидностей обучающих программ и средства широкополосного доступа в Интернет. Компьютерный комплекс ЕМОС предназначен для кардинального увеличения качества образования с помощью внедрения информационных образовательных технологий и применения более безупречных технических средств преподавания и коммуникации.

ЕМОС – это компьютерное комплексное решение, которое состоит из отдельных, аппаратно свободных модулей. Это дает возможность внедрять его как целой группой, так и применять отдельные составляющие решения. Базисный набор состоит из последующих модулей: аппаратно-программный компьютерный комплекс "Методический центр колледжа", аппаратно-программный компьютерный комплекс "Сервер факультета", мобильный компьютерный комплекс, мультимедийный аудиторный компьютерный комплекс, мультимедийный лекционный компьютерный комплекс и предустановленное программное обеспечение. В составе програмного обеспечения: автоматизированная система управления учебным заведением с встроенной системой управления качеством образования, система управления обучением с подсистемой разработки электронных учебных пособий, инструментарий интерактивной доски, программное обеспечение для коллективной работы и для лингафонного офиса, и еще цифровые образовательные ресурсы.

Решение ЕМОС для колледжей всецело подходит для корпоративных образовательных центров, решает подобные задачи и обеспечивает весь перечень возможностей, достаточный для изучения персонала учреждения.

Методический центр колледжа

«Его главное назначение - поддержка постоянного изучения учителей колледжа для увеличения их профессионального уровня хранения и распространение цифровых обучающих ресурсов колледжа. Благодаря ансамблю вероятна совместная исследование учебных программ, отдельных лекций и семинаров и материалов к ним, переподготовка учителей и глав факультетов без отрыва от учебного процесса. "Методический центр колледжа" кроме прочего дает возможность проводить открытые занятия, аттестацию преподавательских и управленческих кадров колледжа. В составе входит – сервер, источник бесперебойного питания, сетевой концентратор, коммуникационный шкаф, интерактивный кабинет-студия для вещания по каналам web-телевидения и в системе дистанционного преподавания, компьютеры для генерации ЦОР и специализированное программное обеспечение "Методический центр колледжа" [12, с.27].

Аппаратно-программный компьютерный комплекс «Сервер факультета».

«Предназначен для поддержки локальных информационно-образовательных сети отдельных факультетов. С поддержкой групп вероятна выкладка, каталогизация и поиск учебных материалов, творение электронной библиотеки материалов и обмен ими меж студентами и учителями. Компьютерный комплекс дает возможность проводить занятия при помощи интерактивных досок в аудиториях, материалов и библиотек, вести видеозапись занятия и сочинять для него каталог материалов, что имеют все шансы, в том числе, быть применены для удаленного преподавания студентов, недостающих в учебном заведении (по болезни или иным причинам). На базе кроме прочего ведутся разные формы проверки студентов.»

«В состав входят сервер, источник бесперебойного питания, сетевой фильтр, коммуникационный шкаф и специализированное программное обеспечение».

Мобильный компьютерный комплекс (МКК)

«Решает важную проблему компьютеризации не очень больших помещений прогрессивным компьютерным оборудованием. Он представляет собой набор ноутбуков (до 25 шт.). Ноутбука большой мощности для учителя (1 шт.) с предустановленной операционной системой Windows 10 и специализированным образовательным ПО коллективной работы. Оптической мышью, гарнитурой, также точкой доступа беспроводной сети, которая хранится в надежной мобильной тележке-сейфе. Кроме штатной точки доступа к беспроводной сети Wi-Fi, МКК быть может опционально укомплектован проектором и функциональным приспособлением, что кроме того хранятся в тележке-сейфе».

«Это дает возможность всего за пару минут организовать высоко оснащённый офис для проведения интерактивных лекций, семинаров, лабораторных и практических работ, демонстраций в любом помещении, в том числе и не предназначенном для работы с компьютерами, по сколько не потребуется включения к сети электропитания и проводной сети передачи данных. При данном тележка-сейф МКК гарантирует защиту оборудования при хранении и перевозке меж аудиториями. Во время хранения ноутбуков их батареи автоматически подзаряжаются».

«Ноутбуки студентов объединяются в беспроводную сеть с выходом в Интернет

Мультимедийный лекционный компьютер (МЛК)

«Предназначен для больших аудиторий и многочисленности студентов (например, при общих лекциях для нескольких факультетов или всего потока). Поэтому кроме функциональности, он дает возможность показывать изображение на большом проекционном экране, увеличивая аудиторию с нескольких десятков до нескольких сотен человек, проводя в интерактивном режиме не лишь учебные события, но и совместные собрания, демонстрации, научные конференции, в том числе и в режиме видеоконференций с другими колледжами и научными организациями».

В состав МЛК кроме оборудования МАК, входят дистанционно управляемый проектор (2500 ANSI люмен, разрешение 1024x768 XGA), дистанционно управляемый проекционный экран (максимальные объемы - ширина 5.2 безвозвратном, высота 4 безвозвратном, диагональ 6.5 м) и система управления освещенностью аудитории (опционально)».

Система управления обучением, подсистема разработки электронных учебных пособий.

«Программная среда, сделанная при интенсивном участии учителей и методистов. Предполагает собой конструктор курсов, лекций и исследований, поддерживает возможность проведения занятий с применением интерактивной доски и способна завозить наружные цифровые образовательные ресурсы. Одна из задач - структурированное хранение учебных материалов, электронных образовательных ресурсов, обучающих программ, литературы в электронной форме и контролируемый доступ к ним. Кроме того, она дает возможность для разного рода коммуникаций между учителем и студентами, в том числе учебных форумов и чатов» [19, с.70].

«Функция отслеживания итогов дает возможность как учителю (или декану), так и студенту в настоящем времени наблюдать за плодами исследований всех уровней сложности, включая экзаменационное тестирование, смотреть статус прохождения курсов. Важно отметить, что доступ к ресурсам в сети Сеть интернет управляем, что дает возможность позволять ознакомление с выбранными учебными и познавательными порталами».

Программное обеспечение кроме того дает возможность отлично организовать дистанционное образование – как учителей, так и студентов.

Система безопасности

«В состав данной системы, встроенной в МИОС, входит подсистема информационной безопасности, цель которой - защита МИОС от нарушения конфиденциальности, а еще доступность, целостность и фильтрация материалов, получаемых из сети Сеть интернет. Она кроме того обеспечивает

аутентификацию пользователей и возможность безопасного удаленного доступа».

«Опционально возможности данной системы имеют все шансы быть значительно расширены с помощью интеграции с подсистемами инженерно-технической и физической безопасности. Подсистема инженерно-технической безопасности состоит из системы учета и контроля инженерных сети и систем, а еще кадастра, и дает возможность контролировать состояние коммуникаций» [14].

Подсистема физической безопасности обладает широким диапазоном полномочий для безопасности людей и имущества. Это быть может и встроенная система управления происшествиями безопасности на территории колледжа, и пожарно-охранная сигнализация, видеонаблюдение, контроль доступа и его интеграция в систему учета успеваемости. Весь данный перечень возможностей контролируется и управляется с единой консоли управления системы безопасности.

2.3 Структура сети

«Локальная сеть. Локальная вычислительная сеть (ЛВС)- это совокупность компьютеров и прочих средств вычислительной техники (активного сетевого оборудования, принтеров, сканеров и т.п.), объединённых при помощи кабелей и сетевых адаптеров и работающих под управлением сетевой операционной системы. Вычислительные сети делаются для того, чтобы группа пользователей имела возможность в сочетании использовать одни и те же ресурсы: файлы, принтеры, модемы, процессоры и т.п. Каждый компьютер в сети обустроен сетевым адаптером, адаптеры соединяются при помощи сетевых кабелей и именно тем связывают компьютеры в единую сеть».

Компьютер, присоединенный к вычислительной сети, называется рабочей станцией или сервером, в зависимости от исполняемых им функций.

Отлично эксплуатировать мощности ЛВС: дает возможность использование технологии («клиент/сервер»). В учреждении применяется ЛВС.

«Прием и предоставление данных в учреждении осуществляется через электронную почту. Электронная почта. Электронная почта (e-mail, от латинского "electronic mail") считается передовым средством передачи информации. В отличие от обычной почты, по электронной почте передаются электронные копии сообщений, файлы, программы, разные данные – т.е. информация, подвергнутая обработке при помощи компьютера».

«Электронная почта - обмен почтовыми сообщениями с любым абонентом сети Internet. Есть возможность отправки как текстовых, так и двоичных файлов. На объем почтового сообщения в сети Internet накладывается последующее лимитирование. «Электронная почта считается более простым средством организации взаимосвязи между удаленными абонентами и может рассматриваться как компьютерный аналог обычной почты. Большая скорость передачи информации и надёжность (при условной цены услуг) позволяют электронной почте отменно поменять роль почтовых служб. Бывает замечена возможность проворно соединить операторов (как бы далеко друг от друга они не находились) с всевозможными документами, планами и т.п. Для хоть какой почты вполне возможно абсолютно в равной степени предположить информационную сущность отправления» [22, с.364]:

- рабочая информация (адреса и др.);
- личное сообщение.

Работа оператора электронной почты на его компьютере производится с внедрением специализированных программ, исполнение которых чередуется. Данные программы исполняют, в соответствии с данными, следующие функции:

- тест полученных сообщений и (или) подготовку новых;
- обмен сообщениями с узлом связи;

Работа первой программы похожа на работу компьютера с текстовой информацией.

Значительное отличие электронной почты от обычной содержится в том, что «отделение связи»» обслуживает лишь наш компьютер: оно практически постоянно в нашем компьютере.

«Отправка сообщений электронной почтой. Ключевыми объектами, основополагающими систему электронной почты, считаются Особые компьютеры, именуемые почтовыми серверами, и компьютеры-клиенты, что обслуживают физических посетителей. Требуемые составляющие данной системы – Специализированные программы и протоколы».

С поддержкой почтовой программы вполне возможно писать сообщения, считывать их с почтового сервера, работать с адресной книжкой, сохранять и организовывать письма в компьютерах "почтового ящика", готовить файлы для пересылки и преобразовывать их в подходящий формат после получение и др.

«С поддержкою почтовой программы оператор делает сообщение адресату, задает адрес, посылает сообщение, после же соединяется с почтовым сервером. Во время соединения почтовый сервер запрашивает имя пользователя и его пароль. Иначе сеанс взаимосвязи не состоится. После соединения приготовленная почта автоматически отправляется на сервер и дальше через передачу от одного к другому почтовому серверу достигает адресата» [32, с.102].

«Почтовые программы Internet дают возможность писать сообщения, находясь в сеансе с сервером, заказывать новинки, сообщать информацию создателям Wed-сайтов. Оператор, получая почту, может в это же время осуществлять поиск информации в сети».

«Пакеты электронной почты исполняют такие функции, как подготовка и обработка слов, чтение, удаление, ввод адресов и тем сообщений, преобразование в необходимый формат отсылаемых файлов. Хоть такой пакет электронной почты имеет интегрированный текстовой редактор для

обработки сообщений. Почти все программы обмениваются словами в кодах ASCII. Но распространены и другие шифровки слов, к примеру, KOI-8. Для пуска пакетов электронной почты Internet Mail, Outlook Express, Exchange Mail, The Bat! и пр. нужно обнаружить пиктограмму программы и щелкнуть на ней указателем мыши» [9, с.82].

«Все почтовые письма, имеющие отношение к данному оператору, хранятся в четырех папках: Входящие, Исходящие, Отправленные, Удаленные. После получения с сервера письмо поступает в папку Входящие. После чтения остается там же, но уже помечается как прочитанное. В папке Удаленные хранятся те сообщения, что были удалены пользователем. В папке Исходящие показываются те письма, что пользователь сделал для отправки. В момент соединения с сервером письмо движется в папку Отправленные. Если сеанс взаимосвязи был неуспешным, тогда письмо остается в папке Исходящие».

«Письма электронной почты могут иметь вложения. Так, на пример, к электронному письму быть может, приложен файл со схемой или же, к примеру, с программой. Форматированные документы, произведенные в текстовом процессоре (например, планы договоров), такие иногда прикладываются к электронному письму».

Электронная почта оказалась во многом удобнее обычной, "бумажной". Не говоря уже о том, что Вам не приходится идти до почтового ящика, чтоб получить или выслать письмо:

1. Электронной почтой письмо в большинстве случаев доставляется значительно быстрее, чем обычной.

2. Стоит это дешевле.

3. Для отправки послания нескольким адресатам не надо печатать его в нескольких экземплярах, достаточно единожды набрать текст в компьютере.

4. Если необходимо перечитать, поправить составленное Вами письмо, или же применять выдержки из него, это сделать проще, потому что текст уже присутствует в машине.

5. Удобнее беречь много писем в файле на диске, чем в ящике стола; в файле проще и искать [1, с.127].

2.4 Защита корпоративной системы в учреждении «Костанайский социально–технический колледж»

Система безопасности в «КСТК» 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 в «КСТК», являются:

Конституция Республики Казахстан (с изменениями и дополнениями по состоянию на 10.03.2017 г.)

Закон РК «Об образовании» от 27 июля 2007 г. №319-III

Приказ Министерства образования и науки РК от 20.04.2011 №152.

Приказ Министра образования и науки Республики Казахстан от 19 ноября 2008 года №613

Приказ Министерства Образования и Науки РК от 23.04.2015 № 230

Постановление Правительства Республики Казахстан от 17.05.2013 № 499

Распоряжение Премьер-Министра Республики Казахстан от 12 февраля 2013 года № 24-р.

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 университете реализованы следующим образом:

– организован контроль, соблюдение временного режима труда и пребывания сотрудников «КСТК» на его территории;

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

– администрирование сети и разграничением прав пользователей. Политика безопасности домена «КСТК» предписывает пользователям регулярно изменять свои пароли, контролирует не повторяемость и непохожесть паролей. В качестве недостатков данного уровня защиты можно указать следующие факты.

В «КСТК» отсутствуют регулярное обучение пользователей информационной системы (ИС), периодические инструктажи, наказания/ поощрения пользователей, что ведет к небрежности пользователей ИС, выраженная в недостаточном знании правил защиты конфиденциальной информации, непониманием необходимости тщательного их выполнения, а у обучающихся, заключающаяся в частоте блокирование системы из-за неправильности введенных данных. Также пока не утверждена на административном уровне политика информационной безопасности.

2 уровень: Программно-аппаратный.

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

В «КСТК» осуществляется управление доступом путем деления информации по соответствующим должностям и полномочиям доступа к ней,

т.е. спецификация и контроль действий пользователей над его информационными ресурсами.

Программно-аппаратные средства защиты информации «КСТК»:

MikroTik RouterBoard hAP, N300 - барьер защиты от атак снаружи, роутер со встроенными сетевыми firewall, dns, vpn, в котором можно открыть или закрыть любые порты, заблокировать доступ на сайты, настроить блокировку сети и интернета итд. Антивирусная система Eset nod endpoint для защиты от компьютерных вирусов, обновление баз и сканирование рабочих станций производится регулярно. Таким образом, можно сделать вывод, что система обеспечения информационной безопасности в «КСТК» существует, но имеет некоторые уязвимости.

Самым уязвим местом в системе безопасности можно назвать сотрудников «КСТК» и программно-аппаратные средства.

2.4.1 Защита автоматизированной информационной системы Platonus

Platonus - это автоматизированная информационная система, позволяющая комплексно автоматизировать процессы кредитной и дистанционной системы изучения. Система имеет централизованную базу данных, в какой отражаются все настоящие действия и процессы колледжа. Для каждого студента и работника учтен, так именуемый, кабинет пользователя (персональная web-страничка), позволяющий автоматизировать работникам колледжа собственные ключевые задачи, студентам видеть требуемую информацию, а дистанционно обучающимся студентам мгновенно получать доступ к кейсам и контролю познаний, онлайн в настоящем времени разговаривать с учителем средством сети интернет Веб или внутренней сети колледжа.»

Возможности:

1. Дистанционное изучение продано как гибрид кейсовой и сетевой технологии обучения.

2. Индивидуальные учебные календари.
3. Система сообщений и назначений заданий дает возможность вести внутреннюю переписку и совершать контроль исполнения заданий.
4. Виртуальные аудитории, включающие просмотр и доступ к УМК (кейсам, лекционным материалам по этому предмету), прохождение испытания и многое другое.
5. Мощная система тестирования.
6. Графическая доска.
7. Общий форум колледжа.
8. Общий чат колледжа.
9. Общая электронная библиотека колледжа.
10. Возможность блокирования доступа студентов и работников (например, за неуплату или административное наказание) [2, с.109]

Виртуальные аудитории.

И уже нет различия между занятием в обычной аудитории и занятием с аудиторией территориально удаленных студентов (от тех, кто посиживает в нескольких метрах от вас, и тех, кто располагается в тысячах километров).

Все это поддерживается технологией Виртуальных аудиторий включающих средства интерактивного обучения:

1. Графическая доска. Доска может помочь вам при помощи мышки рисовать на виртуальной доске (как если б это был графический редактор MS Paint), чтоб объясняемый учителем материал был более ясным и приятным. Изображение с доски передается любому студенту, присоединенному к виртуальной аудитории. Есть возможность «вызвать студента к доске», чтобы студент имел возможность что-нибудь нарисовать на ней (например, решить математическое задание), и еще сделать фоновым рисунком графической доски какой-либо заблаговременно приготовленное изображение (схема, график и т.п.), что вполне возможно переключать в период урока как слайды.

2. Система моментального обмена сообщениями внутри виртуальной аудитории.

3. Система отслеживания информации в виртуальной аудитории.

4. Учебно-методический комплекс по предмету (в форме иерархического дерева материалов по дисциплине), включающий силлабус, лекции и прикрепленные файлы всех форматов (сгруппированные в кейсы).

5. Календарь событий, взаимосвязанный с академическим календарем студента и предстоящими экзаменами, а еще другой календарной информацией.

6. Система контроля знаний

7. Отправка и отслеживание заданий (через подсистему документооборота).

«Общий чат»

Общий чат колледжа позволяет студентам, учителям и прочим пользователям системы сообщаться, не отрываясь от текущих дел. При помощи моментальных сообщений в настоящем времени пользователь системы задает невидимому собеседнику интересующий его вопрос и мгновенно получает ответ».

«Электронная библиотека с системой поиска»

Электронная библиотека дает возможность собирать самый популярный и прогрессивный контент и давать его студентам, учителям и прочим пользователям».

«Управление доступом»

Возможность блокирования доступа студентов и служащих (например, за неуплату или административное наказание) даст возможность использовать административные меры в целях обеспечения значимого выполнения, увеличения ответственности».

«Система проверки (внутри виртуальной аудитории)»

Беспристрастная оценка знаний, непредвзятое отношение к студентам поддерживаются с помощью функциональной системы тестирования.

Случайная подборка вопросов дает любому студенту индивидуальный вариант теста, что исключает возможность совпадения вариантов. По завершении тестирования итоги отправляются на сервер, в тот самый момент автоматически складывается ведомость, и оценки проставляются в журнале».

"PLATONUS" позволяет колледжу прослеживать все учебные процессы, такие как существо академических календарей, распределения учебных дисциплин по учителям, расчет часов по факультетам, запись студентов на элективные дисциплины, существо рентабельных академических потоков, проведения тестирования, механическое составление докладов по различным аспектам и т.д.

Система дает индивидуальные виртуальные офисы (web-страницы):

1. офис регистратору.
2. приемной комиссии.
3. диспетчерской службе
4. отделу кадров.
5. учебной администрации.
6. преподавателю.
7. студенту.

Каждый студент может применять собственный индивидуальный виртуальный офис:

1. Для ознакомления с силлабусами дисциплин и типовым учебным планом.

2. Для регистрации на элективные дисциплины и формирования собственного личного учебного плана.

3. Для просмотра транскрипта и расписания учебных занятий.

4. Для доступа в виртуальную аудиторию.

Виртуальные аудитории, включающие средства интерактивного изучения, такие как графическая доска, система моментального обмена сообщениями, система отслеживания активности в журнале учителя, учебно-методические группы по дисциплинам в форме иерархического дерева

материалов и система контроля знаний, применяют для самостоятельной работы студентов под управлением учителя.

Введение образовательной платформы "PLATONUS" содействует успешной и подходящей организации учебного процесса в колледже.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

Во второй главе нами были рассмотрены текущее состояние защищённости корпоративной информационной системы в Костанайском социально-техническом колледже.

Было изучено становления учреждения, основные направления деятельности в целях подготовки квалифицированных кадров по техническим и социально значимым специальностям, а также изучена структура учреждения.

Проанализированы используемые меры безопасности и предосторожности, текущее состояние защищенности и защита автоматизированной информационной системы Platonus, которая позволяет комплексно автоматизировать процессы кредитной и дистанционной системы обучения.

В третьей главе показаны основания и этапы разработки рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации СПО.

ГЛАВА 3: РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ВЫБОРУ СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1. Общие требования к защите

С целью соблюдения принципа индивидуальной ответственности за собственные действия любому работнику, допущенному к работе с точной подсистемой АС, должно быть сопоставлено персональное неповторимое имя - учетная запись пользователя и пароль, под которым он будет авторизоваться, и работать в системе. Каким-либо работникам, при наличии производственной потребности, могут быть сопоставлены несколько учетных записей. Внедрение несколькими работниками при работе в АС первого и такого же имя пользователя (“группового имени”) ЗАПРЕЩЕНО. создание, изменение и удаление учетных записей, групп безопасности и почтовой рассылки осуществляется лишь по заданию руководства.

Порядок доступа к ресурсам Web.

«Для выполнения задач, связанных с производственной работой сотрудникам предоставляется доступ к ресурсам Web. Требуемый уровень доступа предоставляется работнику на основании заявки «на изменение списков доступа» от управляющего подразделения на имя начальника ИТЦ после ознакомления под роспись о принятых Правилах «Работы в сети Интернет». Доступ к ресурсам интернета может быть блокирована системным администратором без предварительного уведомления, при возникновении нештатных ситуаций, или в других случаях, предусмотренных организационными документами» [31, с.182].

При работе с ресурсами Интернет работнику запрещается:

- загружать и запускать исполняемые или другие файлы без предварительного выяснения на присутствие вирусов установленным антивирусным пакетом;
- использовать неизвестные прокси-серверы;

– использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к применению политикой организации [50, с.91].

Требования к паролям.

Изначальный пароль - позиция знаков (буквы, цифры, знаки препинания, Особые символы), устанавливаемые системным администратором при создании новой учетной записи. Установку изначального пароля создает системный администратор при создании новой учетной записи. Обязанность за сохранность изначального пароля лежит на системном администраторе.

При установке изначального пароля, системный администратор должен установить опцию, требующую смену пароля при первом входе в систему, также уведомить собственника учетной записи о потребности произвести смену пароля.

Основной пароль – позиция знаков (буквы, цифры, знаки препинания, Специализированные символы), распространенная лишь работнику организации, применяемая для доказательства подлинности обладателя учетной записи.

Установку ключевого пароля создает пользователь при первом входе в систему с новой учетной записью.

Пользователь несет индивидуальную ответственность за сбережение в тайне ключевого пароля. Запрещается давать пароль третьим лицам, записывать его, а аналогично пересылать открытым словом в электронных сообщениях.

Пользователь должен не реже одного раза ежемесячно осуществлять смену главного пароля, соблюдая требования.

«Восстановление забытого ключевого пароля пользователя осуществляется системный администратором методом перемены (сброса) главного пароля пользователя на изначальный пароль. На основании письменной или электронной заявки пользователя».

«Для предотвращения подбора паролей системный администратор должен настроить приспособление блокировки учетной записи при трехкратном ошибочном вводе пароля»

«Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки собственника учетной записи».

Администратор пароль – позиция знаков (буквы, цифры, знаки препинания, Особые символы), известная системному администратору (администратору БД, администратору приложения), применяемая при настройке учетных записей, учетных записей служб и сервисов, а аналогично Специализированных учетных записей.

Собственные пароли обязаны подходить грядущим требованиям:

1. Длина пароля обязана быть более 8 символов.

2. В числе знаков пароля обязаны существовать буквы в верхнем и нижнем регистрах, цифры и специализированные знаки (@, #, $, &, *, % и т.п.).

3. Пароль не обязан включать в себя просто вычисляемые сочетания знаков (имена, имени, названия АРМ и т.д.), а еще общепризнанные уменьшения (ЭВМ, ЛВС, USER и т.п.).

4. При смене пароля новое значение обязано отличаться от предшествующего минимум, чем в 6 позициях.

5. Личный пароль пользователь не имеет права сообщать никому [26, с.18].

3.2 Защита информации в компьютерных сетях

«Наличие многократных или временных физических соединений считается главнейшим моментом, который оказывает большое влияние на увеличение уязвимостей систем вследствие брешей в применяемых

защитных и программных средствах и утечки информации вследствие ложных и неграмотных деяний персонала».

Обеспечение требуемой защиты информационных компьютерных в данных условиях достигается применением дополнительных инструментальных средств.

К их числу относятся:

1. Средства анализа безопасности операционных систем и сетевых сервисов.

2. Средства обнаружения небезопасных информационных действий (атак) в сетях.

Средства анализа безопасности операционных систем позволяют воплощать в жизнь проверку приспособлений разграничения доступа. Иидентификации и аутентификации, средств прогноза, аудита, и прочих компьютерных операционных систем, с другой стороны медали соотношения их опций, и конфигурации установленным в организации.

«Кроме этого, средствами этого класса ведется контроль целостности и неизменности программных средств и системных установок и ревизия присутствия уязвимостей системных и прикладных служб. Как правило, такие выяснения ведутся с внедрением информационной базы уязвимостей операционных систем и сервисных служб, что могут обновляться по мере выявления новых уязвимостей».

«Использование в сетях Internet протоколов TCP/IP, что характеризуются наличием в них неустранимых уязвимостей, привело к выходу в свет в последнее время новых видов информационных действий на сетевые сервисы и представляющих настоящую угрозу безопасности информации. Средства анализа безопасности сетевых сервисов используются для оценки безопасности компьютерных сети по отношению к внутренним и наружным атакам. По итогам анализа безопасности сетевых сервисов средствами генерируются отчеты, включающие в себя перечень выявленных уязвимостей, описание вероятных опасностей и советы по их уничтожению.

Поиск уязвимостей основывается на применении базы этих, которая имеет обширно именитые уязвимости сетевых сервисных программ и может обновляться методом добавления новых уязвимостей» [32, с.108].

К числу средств анализа этого класса относится программа SATAN (автор В.Венема), Netprobe Qualix Group и Internet Scanner Internet Security Systems Inc.

Наибольшая эффективность защиты информации достигается при комплексном применении средств анализа безопасности и средств обнаружения небезопасных информационных действий (атак) в сетях. Средства обнаружения атак в сетях созданы для претворения в жизнь контроля всего сетевого трафика, который проходит через защищаемый сектор сети, и оперативного реагирования нападения на узлы сети.

Большинство средств этой группы при обнаружении атаки в сети оповещают администратора системы, обращают внимание прецеденты нападения в журнале системы и заканчивают соединение с атакующим узлом. Вдобавок отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы сети.

Защита компьютерных сети на 4 уровнях модели ISO/OSI.

«Средством обеспечение информационной поддержки компьютеров в основном количестве случаев считается его компьютерная сеть. Голосовая телефония, радиосвязь, факс и обычная почта рассматривается сообща с компьютерными сетями т.к. их средства без компьютерных технологий в значительной степени ограничены ».

Модель ISO/OSI.

«Особенности охраны компьютерных сетей описаны семиуровневой моделью взаимодействия открытых систем (Open Systems Interconnection, OSI), созданная интернациональным комитетом по стандартизации ISO. В согласовании с концептуальными положениями данной модели процесс информационного обмена в компьютерных сетях вполне возможно поделить

на 7 рубежей в зависимости от того, каким образом, и меж какими объектами наблюдается информационный обмен. Любому уровню модели соответствует некая группа стереотипов и спецификаций. Рассмотрим специфики обработки информации на физическом, канальном, сетевом и автотранспортном уровнях. По любому уровню будут представлены сведения о уязвимостях приспособлений информационного взаимодействия, отличительных для этого уровня и советы по уничтожению данных уязвимостей» [20, с.198].

Физический уровень.

«Самый маленький уровень модели взаимодействия открытых систем обрисовывает процессы, происходящие на физическом уровне или же уровне среды передачи».

«Обеспечить безопасность информационного обмена на физическом уровне модели вполне возможно с помощью структуризации физических связей меж узлами компьютерной сети. Защищенная физическая среда передачи этих считается первым рубежом для злоумышленника или же преградой для действия и разрушительных моментов окружения».

Главные советы позволяющие понизить возможность эксплуатации кабельной системы компьютерной сети фирмы злоумышленником.

1. «Рекомендуемая конфигурация физических связей в компьютерной сети фирмы – «звезда», при всем этом для включения каждого узла выделен отдельный кабельный сектор. В качестве среды передачи употребляется восьмижильный медный кабель вида «витая пара» или оптоволокно».

2. «Для включения критически актуальных для компьютерных серверов применяют два кабельных сектора – главный и резервный».

3. «Прокладка сетевого кабеля осуществляется в тайной электропроводке, или в закрываемых кабель - каналах с вероятностью опечатывания не срываемыми наклейками – «стикерами».

4. «Кабельные разделы, применяемые для включения всех узлов компьютерной сети, обязаны быть сконцентрированы на одной коммутационной панели».

5. Коммутационная панель смонтирована в запираемом коммутационном шкафу. Доступ в здание коммутационного шкафа строго ограничен и контролируется службой безопасности учреждения [36, с.18].

Канальный уровень.

«Обеспечение безопасности разделения среды передачи коммуникационными средствами канального уровня. Протоколы и стереотипы этого уровня обрисовывают процедуры ревизии доступности среды передачи и корректности передачи этих. Подавляющая большая часть компьютерных сети выстроено на базе технологий Ethernet, Fast Ethernet b Gigabit Ethernet. Преступник может выполнить прослушивание трафика произвольно подобранной парой узлов компьютерной сети. Советы, что позволяют вдобавок уберечь компьютерную сеть компании средствами канального уровня».

1. «Администратор службы безопасности обязан вести инвентаризационную ведомость соотношения аппаратных и сетевых адресов всех узлов сети учреждения».

2. «Средства коммутации канального уровня, применяемые в компьютерной сети фирмы, обязаны быть настраиваемыми и обеспечивать разграничение доступа меж узлами сети согласно с разработанной политикой».

3. «Администратор сети обязан выполнить настройку для реализации разработанной защиты. В обязанности администратора входит кроме прочего отключение неиспользуемых подсистем коммутатора».

4. «Администратор сети обязан периодически контролировать соотношение конфигураций коммутаторов разработанной политическом деятеле защиты».

5. «Администратор сети обязан вести прогноз сетевой активности пользователей с целью выявления источников аномально высочайшего численности широковещательных запросов».

6. «Служба безопасности обязана обеспечить жесткий контроль доступа в помещения, в каких размещены коммутаторы и рабочие станции, с которых дополнительно допустимо управление коммутаторами» [40, с.13].

Сетевой уровень.

Применение в компьютерной сети протоколов сетевого уровня считается достаточным условием для обеспечения взаимодействия меж узлами сети с всевозможными канальными протоколами. Сетевые протоколы позволяют одолеть лимитирования, накладываемые спецификациями канального уровня. В основной массе случаев администратор и служба безопасности фирмы не имеют возможности вполне проверить узлы подключаемой сети, и значит, формализовать правила обмена пакетами канального уровня.

Одной из задач администратора сети и считается защита адресного места сети от возможности его применения злоумышленником. Частично данную функцию исполняют механизмы маршрутизации, реализованные модулями протокола сетевого уровня. Решение проблемы бесспорно – надо применять все адресное пространство и вовсе не уяснить злоумышленнику возможности завладеть адреса неиспользуемых узлов.

Транспортный уровень.

«Применение транспортных протоколов позволяет создать более эффективную преграду работы злоумышленника. Тут для защиты употребляются находящиеся в заголовках частей (сегмент – блок этих с которыми действует транспортный протокол) транспортного протокола. Администратор сформировывает систему деятельности защиты сети средствами транспортного уровня в форме ведомости соотношения хостов, применяемых ими сетевых адресов и доверенных добавлений,

функционирующих на платформах данных хостов. Формализованная запись данной ведомости представляет собой табличную структуру, содержащую»:

- перечень узлов (хостов), их символьные имена;
- соответствующие данным узлам (хостам) сетевые адреса;
- перечень применяемых любым узлом (хостом) транспортных протоколов;
- перечень сетевых добавлений, функционирующих в каждом узле и надлежащие данным приложениям порты транспортного протокола;
- по любому сетевому приложению нужно будет установить, считается ли оно покупателем или поставщиком ресурса, т.е. дополнительно допустимо ли ему инициировать исходящие соединения или же воспринимать входящие [32, с.162].

«Реализация защиты средствами транспортного уровня осуществляется при помощи межсетевых экранов (firewall). Межсетевой экран — это специализированное программное обеспечение, реализующее фильтрацию трафика согласно с правилами защиты сети средствами транспортного уровня».

«Методика Firewall в общем случае методика Firewall как главное программно-аппаратное средство воплощения сетевой защиты безопасности в выделенном разделе IP-сети продает следующие главные функции».

1. Многоуровневая фильтрация сетевого трафика.

Фильтрация традиционно наблюдается на 4 уровнях OSI:

Канальном (Ethernet). Сетевом (IP). Автотранспортном (TCP, UDP). Прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация сетевого трафика считается главный функцией систем Firewall и дает возможность администратору безопасности сети централизованно воплощать в жизнь требуемую сетевую систему деятельности в выделенном секторе IP-сети, настроив надлежащим образом Firewall, вполне возможно дополнительно пустить или запретить пользователям как доступ из внешней сети к подходящим службам хостов

или же к хостам, оказавшимся в защищаемом разделе, так и доступ пользователей из внутренней сети к подходящим ресурсам внешней сети. Вполне возможно провести аналогию с администратором локальной сети. Который для претворения в жизнь защиты безопасности в системе назначает требуемым образом сообразные дела между субъектами (пользователями) и объектами системы (файлами, например), что дает возможность разграничить доступ субъектов системы к ее объектам согласно с установленными администратором правами доступа. Те же размышления применимы к Firewall-фильтрации: в роли субъектов взаимодействия будут выступать IP-адреса хостов пользователей, ну а в качестве объектов, доступ к которым нужно разграничить, - IP-адреса хостов, применяемые автотранспортные протоколы и службы предоставления удаленного доступа.

2. Proxy-схема с положительной идентификацией и аутентификацией пользователей на Firewall-хосте «Proxy-схема дает возможность, во-первых, при доступе к защищенному Firewall разделу сети выполнить на нем дополнительно идентификацию и аутентификацию удаленного пользователя и, во вторых, считается основой для создания частных сети с виртуальными Айпи адресами. Значение proxy-схемы содержится в создании соединения с конечным адресатом через переходный proxy-сервер (в переводе с англ. "proxy" - полномочный) на хосте Firewall».

3. Существование частных сети с "виртуальными" Айпи адресами

Если администратор безопасности сети считает целесообразным скрыть настоящую топологию собственной внутренней IP-сети, тогда ему вполне возможно посоветовать применять системы Firewall для создания виртуальной сети с применением технологии NAT (Network Address Translation). Для адресации в наружную сеть через Firewall нужно будет или применять на хосте Firewall описанные выше proxy-серверы, или использовать исключительно Особые системы маршрутизации (через что и вероятна наружная адресация). Это наблюдается вследствие того, что применяемый во внутренней частной сети "виртуальный" Айпи адрес,

неоспоримо, непригоден для внешней адресации, другими словами адресации к абонентам, окружающим за ее пределами. Вследствие этого proxy-сервер обязан совершать взаимосвязь с абонентами из внешней сети со собственного истинного IP-адреса. что, данная схема комфортна в том случае, если вам для осуществления IP-сети подчеркнули недостающее число IP-адресов: в эталоне IPv4 это приключается сплошь и рядом, вследствие этого для настоящей IP-сети с внедрением proxy-схемы достаточно первого выделенного IP-адреса для proxy-сервера.

Наконец, хоть какой прибор, реализующий даже один из данной функций Firewall-методики, и считается Firewall-устройством. К примеру, ничто не мешает вам применять в роли Firewall-хоста компьютер с обычной ОС FreeBSD или же Linux, у которой надлежащим образом необходимо скомпилировать ядро ОС. Firewall этого вида будет обеспечивать лишь многоуровневую фильтрацию IP-трафика. Другое дело – предлагаемые на рынке сильные Firewall-комплексы, разработанные на базе ЭВМ или же мини-ЭВМ, обычно продадут все функции Firewall-методики и считаются полнофункциональными системами Firewall.

«Но Firewall не классифицируется залогом безусловной защиты от удаленных атак в Internet. Данная система - не столько средство обеспечения безопасности, какое количество возможность централизованно воплощать в жизнь сетевую систему деятельности разграничения удаленного доступа к ресурсам вашей сети. Да, в том случае, в случае если, к примеру, к этому хосту запрещен удаленный TELNET-доступ, Firewall несомненно предотвратит возможность этого доступа» [44, с.126].

3.3 Антивирусы

При работе с прогрессивным индивидуальным компьютером пользователюwebля может подстерегать большое количество неприятности: утрата этих, зависание системы, выход из строя отдельных частей

компьютера. Одной из обстоятельств данных задач вместе с промахами в программном обеспечении и неумелыми поступками самого оператора ПЭВМ имеют все шансы быть проникшие в систему компьютерные вирусы .

Для защиты от вирусов вполне возможно использовать:

- общие средства защиты информации, что могут быть полезны кроме того как страховка от физической порчи дисков, неверно работающих программ или же ложных действий пользователей;
- профилактические меры, позволяющие снизить возможность заражения вирусом;
- специализированные программы для защиты от вирусов.

Единые средства защиты информации могут быть полезны не лишь для защиты от вирусов. Есть 2 ключевые разновидности данных способов защиты:

- резервное копирование информации, т.е. создание копий файлов и системных областей дисков на дополнительном носителе;
- «разграничение доступа, предотвращающее несанкционированное внедрение информации, в частности, защиту от перемен программ и этих вирусами, неверно работающими программами и ложными действиями пользователей» [50, с.109].

Несмотря на то, что единые средства защиты информации чрезвычайно существенны для защиты от вирусов, все-таки их мало. Необходимо использовать специализированные программы для защиты от вирусов. Данные программы вполне возможно поделить на несколько видов:

- «программы – сенсоры позволяют обнаруживать файлы, инфицированные одним из нескольких распространенных вирусов»;
- «программы – доктора, или фаги, возобновляют инфицированные программы, убирая из них тело вируса, т.е. программа ворачивается в тогда состояние, в каком она пребывала до инфецирования вирусов»;

– «программы – ревизоры предварительно запоминают сведения о состоянии программ и системных областей дисков, а потом сопоставляют их состояние с начальным. При выявлении несоответствий про это рассказывается пользователю»;
– «доктора – ревизоры – это модификации ревизоров и медиков, т.е. программы, что не исключительно обнаруживают перемены в файлах и системных областях дисков, ведь и имеют все шансы автоматом возвращать их в начальное состояние»;
– «программы – фильтры размещаются резидентно в своевременной памяти компьютера, перехватывают те обращения к операционной системе, что применяются вирусами для размножения и нанесения ущерба, информируют о них пользователю. Пользователь может пропустить исполнение подходящей операции» [26, с.70].

Ни один вид антивирусных программ по отдельности не мешает уверенностью защиты от вирусов. В следствии этого лучшей стратегией защиты от вирусов считается многоуровневая защита.

Средствами в защите от вирусов считается программы – сенсоры, позволяющие проводить проверку снова приобретенное программное обеспечение на наличие вирусов.

На первом уровне защиты пребывают программы для защиты от вируса. Данные программы имеют все шансы первыми сказать о вирусной атаке и избежать инфицирование программы и диска.

Второй уровень защиты создают программы – ревизоры, программы – доктора и докторы – ревизоры. Ревизоры обнаруживают нападение в тех случаях, когда вирус смог пройти через первый уровень. Программы – доктора используются для восстановления инфицированных программ, если ее копий нет в архиве, но они не постоянно врачуют без ошибок. Доктора – ревизоры обнаруживают нападения вируса и лечат инфицированные файлы, при этом осуществляют контроль верность лечения.

Третий уровень защиты – это средства разграничения доступа. Они не позволяют вирусам и ошибочно работающим програмах, в том числе если они внедрились в компьютер, испортить важные данные. В резерве пребывают архивные копии информации и эталонные диски с программными продуктами. Они позволяют возобновить информацию при ее повреждении на жестком диске.

Среди более известных антивирусных пакетов пренадлежит отметить ESET NOD, Kaspersky Antivirus, DrWeb. Перечисленные средства могут сделать хорошую поддержку в обнаружении вирусов и восстановлении испорченных файлов, но важно и соблюдение сравнимо обычных инструкций антивирусной безопасности:

- следует игнорировать воспользоваться незаконными источниками получения программ. Менее же опасен законный прием покупки фирменных продуктов;
- осторожно стоит относиться к программам, приобретенным из сети Internet, потому что нередки случаи инфицирования вирусами программ, распространяемых по электронным каналам связи;
- всякий раз, когда дискета (диск, флешка) побывала в чужом компьютере, нужно проверить дискету при помощи 1-го или же 2 антивирусных средств;
- необходимо прислушиваться к информации о вирусных заражениях на компьютерьютерах в собственном регионе проживания или же работы и о более радикальных средствах борьбы с ними.

В колледже для удаления вирусовов в системе используется антивирусная система ESET NOD.

ESE TNOD разработан фирмой ESET считается одним из фаворитов среди антивируссного программного обеспечения. При испытании показывает высшую скорость нахождения вирусов, а конкретно данный показатель у него лучше других антивирусов. Кроме этого ESET NOD отличается высочайшей скоростью работы, обладает всеми передовыми

средствами защиты компьютеров. В наличии достаточно легкий интерфейс, принцип возможность нередких обновлений, большое количество функций, реализованных на достаточно высочайшем уровне.

По эффектом испытания интернет изданий мира «Virus Bulletin» он признан лучшим. По сопоставлению с Антивирусом Касперского он сканирует в 10 раз быстрее, кроме того с наилучшим эффектом. Его монитор не замедляет функциональность системы.

Плюсы. Высокая скорость работы, потребляет маленькое число ресурсов компьютера, частое обновление сигнатур. Минусы. неимение поведенческого блокиратора.

3.4. Защита электронной почты

Почтовые системы фирмы бывают в опасности. В данное время спам составляет более 50% всех почтовых сообщений, и одно из 30 сообщений имеет вирус или же компьютерьютерного «червя». Данные вредные программы не исключительно причиняют настоящий вред, но и тратят ресурсы процессора. Перегружают каналы взаимосвязи, занимают место на жестком диске и отнимают у пользователей время.

«Создатели принимают меры, пытаясь затормозить поток мусора и наказать создателей непрошенных писем, но проблема становится все остреее и нет ожидания смягчить ее в близком будущем. Защита и восстановление серверов электронной почты от нападений – первоочередная проблема каждого сетевого администратора».

Решения проблемы.

Только в последние пару лет поставщики стали предлагать комбинированные решения для защиты почты, в каких соеденены функции поиска вирусов, блокировки спама и фильтрации контента. Современные защиты располагают последующими возможностями:

- сканирование и тест в настоящем времени;

- наличие информационной базы сигнатур небезопасных программ;
- управление карантином;
- эвристический тест для распознавания найденных раньше угроз;
- работа с одним или же несколькими протоколами или же портами;
- централизованное управление, мониторинг и подготовка отчетов;
- ежедневное обновление сигнатур небезопасных программ;
- оповещение конечных пользователей;
- высокая точность;
- круглосуточные консультации без выходных [5, с.182].

В колледже для выполнения задач, связанных с производственной работой работникам предоставляется доступ к системе электронной почты. Электронная почта считается собственностью фирмы и применяется лишь в рабочих целях. Внедрение электронной почты в иных целях категорически запрещено. Содержимое электронного почтового ящика работника быть может проверено без предварительного уведомления по просьбе конкретного или вышестоящего управляющего.

Системный администратор каждый день проводит тест системы обмена электронной почтой и не реже 1-го раза еженедельно дает статистический доклад о функционировании системы начальнику ИТЦ.

Для безопасности с работой электронной почты запрещается:

- использовать адрес корпоративной почты для подписок;
- публиковать собственный адрес или адрес иных служащих фирмы на общедоступных Web ресурсах (форум, конференции);
- отправлять письма с вложенными файлами единый размер которых превосходит 200 Мегабайт;
- открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, в том числе и если отправитель послания прекрастно известен;

- осуществлять глобальную рассылку почтовых сообщений (более 10) наружным адресатам без их согласия. Эти действия квалифицируются как спам и считаются незаконными;
- осуществлять групповую рассылку почтовых сообщений маркетингового характера;
- рассылка через электронную почту материалов, имеющих вирусы или иные компьютерьютерные коды, файлы или программы, созданные для нарушения, устранения или лимитирования функциональности всякого компьютерного или же телекоммуникационного оборудования или же программ, для организации несанкционированного доступа, также серийные номера к платным программным продуктам и программы для их генерации, логины, пароли и пр средства для получения несанкционированного доступа к коммерческим ресурсам в Интернете, и еще ссылки на вышеуказанную информацию;
- распространение защищаемых авторскими правами материалов, затрагивающих некоторый патент, торгашескую марку, платную тайну, авторские права или же многие другие права принадлежности и/или авторские и соседние с ним права третьей стороны;
- распространять информацию содержание, которой запрещены интернациональным законодательством включая материалы, носящие вредную, угрожающую, клеветническую, безнравственную информацию, а еще информацию, оскорбляющую честь и достоинство иных лиц, материалы, способствующие разжиганию государственной розни, подстрекающие к насилию, призывающие к совершению противоправной работы, в том числе разъясняющие порядок использования взрывчатых веществ и другого пистолета, и т.д.;
- распространять информацию урезанного доступа, представляющую платную тайну;

– предоставлять, кому бы-то ни было пароль доступа к собственному почтовому ящику [7, с.92].

3.5 Рекомендации по улучшению системы защиты информации

В развитии компьютерной техники и программ колледжы и университеты выиграли основную роль. В них разрабатываются, испытываются и внедряются передовые планы в области IT. С подъемом киберпреступности защита конфиденциальной информации и разработок в учебных учреждениях становится особо своевременной.

«Колледжи - инфраструктура, владеющая очень большим банком этих, содержащим информацию различного рода. Это не исключительно учебные методички в электронном форме, но и актуальные проектно-исследовательские выработки. Подъем правонарушений в области больших технологий устанавливает собственные требования к защите ресурсов вычислительных сети учебных заведений и ставит задачку возведения личной встроенной системы безопасности». Ее решение представляет присутствие нормативно-правовой базы, составление концепции безопасности, разработку событий, проектов и процедур по не опасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в масштабах образовательного учреждения. Данные компоненты характеризуют единую систему деятельности обеспечения безопасности информации в колледже.

Специфика защиты информации в образовательной системе содержится в том, что колледж - общественное заведение с непостоянной аудиторией, и еще место завышенной активности "начинающих онлайн преступников". Ключевую группу возможных нарушителей тут оформляют студенты, какие-или из них имеют достаточно высочайший уровень познания персонального компьютера, сети. Возраст - от 18 до 23 лет - и юношеский максимализм вдохновляет этих людей блеснуть познаниями перед

сокурсниками: сделать вирусную эпидемию, получить административный доступ и "наказать" учителя, заблокировав выход в Сеть интернет. Учащиеся имеют доступ лишь в компьютерьютерные учебные аудитории, от них и исходит внутренняя угроза. Работа студентов, учителей в этих аудиториях обязана быть регламентирована приказом (актом) руководством колледжа. Во избежание занесения вредной информации во внутреннюю сеть предпочтительно, чтоб в компьютерьютерах отсутствовали дисководы и были отключены usb-порты.

Тест опасностей, их источников и рисков.

Компьютерные сети образовательных заведений - это совокупность сетевых ресурсов для учебной работы, сотрудников станций персонала, приборов функционирования сети в целом.

Источниками вероятных опасностей информации являются: компьютеризированные учебные аудитории, в которых наблюдается учебный процесс; Интернет; рабочие станции неквалифицированных в области ИБ сотрудников колледжа.

Тест информационных рисков вполне возможно поделить на следущие этапы:

1. Классификация объектов, подлежащих защите, по важности.

2. Определение привлекательности объектов защиты для взломщиков.

3. Определение вероятных опасностей и потенциальных каналов доступа на объекты.

4. Оценка существующих мер безопасности.

5. Определение уязвимостей в защите и методов их ликвидации.

6. Составление ранжированного перечня угроз.

7. Оценка убытка от НСД, атак в отказе обслуживании, сбоев в работе оборудования [6, с.59].

Главные объекты, нуждающиеся в защите от НСД:

1. Бухгалтерские ЛВС, эти планово-финансового отдела, также статистические и архивные данные.

2. Серверы баз данных.

3. Консоль управления учетными записями.

4. www://ftp сервера;

5. ЛВС и серверы исследовательских планов.

Регламент работы.

Для аутентификации пользователей и сотрудников преподавательского персонала, компьютерах в учебных аудиториях вполне возможно использовать ролевое управление доступом (РУД). Сущность технологии - в существе какой-то роли, связывающей пользователя и его привилегии в системе. С ее поддержкою вполне возможно отлично выстроить гибкую систему деятельности разграничения доступа в многопользовательской системе.

«РУД значительно упрощает администрирование многопользовательских систем методом установления связей меж "ролями" и пользователями. Для каждого пользователя быть может активизировано сразу несколько "ролей", что в этоже время имеют все шансы быть приписаны незамедлительно нескольким пользователям».

«Применение сетевой операционной системы Novell Netware дает возможность централизованно править ходом идентификации пользователю в единой сети колледжа, отслеживать их действия, ограничивать доступ к ресурсам. Средства защиты информации (СЗИ) уже интегрированы в данную ОС на базисных уровнях и вовсе не считаются надстройкой в форме некоторого прибавления» [11, с.430].

ОС Novell NetWare имеет механизмы защиты последующих уровней:

1. Защита информации о пользователе.

2. Защита паролем.

3. Защита каталогов.

4. Защита файлов.

5. Межсетевая защита.

Для каждого зарегистрированного в данной ОС пользователя присутствуют правила с указанием списка ресурсов, к которым он имеет доступ, права на работу с ними. Для поддержки администратору работает консоль управления учетными записями. Есть возможность лимитирования права пользователя на вход в сеть временем, датой и точными рабочими станциями. В качестве системы разграничения доступа применяются ACL и контексты. Для каждого контекста определен перечень легкодоступных ресурсов сети. Это дает возможность делить доступ к ресурсам меж администрацией, работниками колледжа и студентами. Кроме того, вполне возможно устанавливать дополнительно массовые защиты в масштабах особого контекста (дополнительноустим, поделить доступ студенческого контекста по факультетам, не используя подконтексты). Интегрированные средства обнаружения и предотвращения атак позволяют резко выявить нарушителя.

«Часто в колледже разворачивается беспроводная сеть, доступ в которую обычно считается независимым. Применять эту схему нужно в том случае, когда точки беспроводного доступа не подключены к внутренней сети колледжа. Как правило, взаимосвязь с Интернетом осуществляется сразу по нескольким линиям взаимосвязи (оптоволоконная линия, спутниковые и радиоканалы). Отдельные каналы предоставляются для взаимосвязи с иными уколледжами или же для не опасного обмена данными. Чтобы ликвидировать опасности, связанные с утечкой и порчей передаваемой информации, такие сети не нужно подключать к масштабным сетками и единой сети» [18, с.152].

Критически главные узлы для обмена данными колледжа (бухгалтерская ЛВС) кроме прочего обязаны присутствовать в отдельности.

Психологические барьеры защиты.

1-ый психологический барьер защиты от атак снаружи (Интернет) – роутер (маршрутизатор). Он используется для взаимосвязи участков сети друг с другом, и еще для более действенного разделения трафика и применения других путей меж узлами сети. От его опций находится в

зависимости функционирование субсетей и взаимосвязь с масштабными сетями (WAN). Его основная миссия в проекте безопасности -защита от распределенных атак в отказе обслуживания (DDOS).

Вторым рубежом может работать МСЭ: аппаратно-программный компьютерлекс Cisco PIX Firewall.

Далее пренадлежит DMZ. В данной зоне нужно разместить крупнейший прокси-сервер, dns-сервер, www/ftp, mail сервера. Прокси-сервер обрабатывает запросы от сотрудников станций учебного персонала, серверов, не присоединенных напрямую к роутеру, и фильтрует трафик. Начальника безопасности на данном уровне обязана определяться блокированием ненужного трафика и его экономией (фильтрация мультимедиаконтента, iso-образов, блокировка страниц нежелательного/нецензурного содержания по основным словам). Чтобы не произашло скачивание зараженной вирусами информации, на данном сервере оправдано размещение антивируса (например, ClamAV). Для более детализированного анализа и контроля трафика пренадлежит использовать IDS (такую, как Snort).

«Информация от прокси-сервера вдоль отсылается на сервер статистики, где вполне возможно понаблюдать и изучить работу пользователей в Сети интернет. На почтовом сервере непременно обязан находиться почтовый антивирус, к примеру, Kaspersky AntiVirus for Mail servers».

Так как данные серверы соединены именно напрямую с глобальной сетью, аудит программного обеспечения, установленного на них, - первоочередная задача инженера по информационной безопасности колледжа. Для экономии средств и эластичности настраивания предпочтительно использовать opensource-ОС и программное обеспечение. Самая известная ОС - FreeBSD и GNU Linux. Но ничто не вредит применять и более консервативную Open BSD или в том числе и сверхстабильную ОС настоящего времени QNX.

Спрос на антивирусные средства выростает с каждым годом и он не обошел инфраструктуру колледжей.

Для централизованного управления антивирусной работой нужен продукт с клиент-серверной частью, такой как Dr.Web Enterprise Suite. Он дает возможность централизованно править опциями и обновлением антивирусных баз при помощи графической консоли и давать удобную статистику о вирусной работы, если таковая присутствует.

Для наибольшего удобства сотрудников колледжа вполне возможно организовать доступ к внутренней сети колледжа при помощи технологии VPN.

Некоторые колледжа имеют собственный пул дозвона для выхода в Сеть интернет и примут на вооружение каналы взаимосвязи учреждения. Во избежание применения этого доступа чужими лицами в преступных целях сотрудники учебного заведения не обязаны разглашать телефонный аппарат пула, логин, пароль.

Степень безопасности сети и серверов основной массы колледжей оставляет хотеть лучшего. Обстоятельств тому немало, но один из основных – скверная организация мер по исследованию и обеспечение защиты информационной безопасности. Управление просто недооценивает значимости данных событий. вторая несогласованность содержится в том, что ни страна, ни администрация колледжа не заинтересованы в выделении средств на закупку оборудования и введение новых технологий в области ИБ.

Предлагается утвердить систему деятельности информационной безопасности.

Предметом защиты информационной безопасности является:

1. Порядок доступа к информационным системам, обрабатывающим конфиденциальную информацию.

2. Работа в сети интернет.

3. Сетевая безопасность.

4. Локальная безопасность.

5. Физическая безопасность (доступ в помещения).

6. Обеспечение защиты индивидуальных данных

7. Дублирование, резервирование и хранение информации [29, с.56].

Совместные положения.

Цели и задачи. Целью данной Защиты считается обеспечение безопасности объектов защиты колледжа от всех видов опасностей, наружных и внутренних, умышленных и непреднамеренных, минимизация убытка от вероятной реализации опасностей безопасности.

Направление информационной безопасности сделано в отделе своей безопасности со последующими задачами и функциями:

1. «Планирование, согласование и организация событий по защите информации именно на объектах информатизации, на которых ведутся работы с внедрением конфиденциальной информации».

2. «Определение полномочий несанкционированного доступа к информации, ее ликвидирования или преломления, определение вероятных технических каналов и тест рисков утечки конфиденциальной информации, исследование подходящих мер по защите.

3. Организация технической защиты информации, роль в существе систем защиты.

4. Проведение периодического контроля состояния ИБ, учет и тест последствий с выработкой решений по уничтожению уязвимостей и нарушений.

5. Контроль за внедрением замкнутых каналов взаимосвязи и ключей с цифровыми подписями.

6. Организация плановых проверок режима защиты, и исследование подходящей документации, тест последствий, расследование нарушений.

7. Разработка и воплощение событий по охране индивидуальных данных

8. Организация взаимодействия со всеми текстурами, участвующими в их обработке, исполнение требований законодательства к информационным

системам, обрабатывающим индивидуальные эти, контроль постукомпьютераов операторов, отвечающих за их обработку.

9. Организационно-правовой статус служащих по обеспечению информационной безопасности [39, с.182].

Работники имеют право беспрепятственного доступа во все помещения, где установлены тех. средства с Информационными системами (ИС), право настоятельно просить от управления подразделений и администраторов ИС остановки автоматизированной обработки информации, индивидуальных данных, при наличии конкретной опасности защищаемой информации;

«Имеют право получать от пользователей и администраторов нужную информацию связанных с использования информационных технологий, в части касающейся вопросов информационной безопасности»;

«Основной эксперт по ИБ имеет право проводить аудит работающих и возобновил внедряемых ИС на предмет реализации требований защиты и обработки информации воспрещать их использование, в случае если не отвечают притязаниям или продолжение эксплуатации может привести к суровым результатам в случае реализации ощутимых опасностей безопасности»;

«Работники имеют право контролировать выполнение подтвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности».

Область действия.

Требования реальной Защиты распространяются на всех работников колледжа (штатных, временных, работающих по договору и т.п).

Порядок доступа к информационным системам, обрабатывающим конфиденциальную информацию.

Система управления доступом к информационным системам при помощи штатных средств (операционных систем (MS Windows Server,

Linux), ИС и применяемых ими СУБД) и создана для реализации последующих функций:

1. Идентификации и проверка подлинности субъектов доступа при входе в ИС.

2. Идентификации терминалов, узлов сети, каналов взаимосвязи, наружных приборов по закономерным именам.

3. Идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

4. Регистрации входа (выхода) субъектов доступа в систему (из системы), или регистрация загрузки и инициализации операционной системы и ее останова.

5. Регистрации доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

6. Регистрации доступа программных средств к терминалам, каналам взаимосвязи, программам, томам, каталогам, файлам, записям, полям записей.

Порядок доступа, получения логинов и паролей, ориентируется Порядком предоставления прав доступа.

Сетевая безопасность.

Доступ из Web в сеть колледжа:

1. Во внутреннюю сеть доступ снаружи запрещен.

2. Как исключение доступ разрешен лишь к определяемым объектам по постановлению директора ЦИТ.

Маршрутизаторы и межсетевые экраны.

Система межсетевого экранирования создана для реализации последующих функций:

1. Фиксации во внутренних журналах информации о проходящем открытом и перекрытом IP-трафике.

2. Идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ.

3. Контроля целостности собственной программной и информационной части.

4. Фильтрации пакетов протоколов, служащих для диагностики и управления работой сетевых устройств.

5. Фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов.

6. Блокировка доступа не идентифицированного объекта или же субъекта, подлинность которого при аутентификации не подтвердилась, способами, устойчивыми к перехвату.

7. Контроля сетевой активности прибавлений и обнаружения сетевых атак.

Для анализа безопасности ИС используются специализированные программно-аппаратные средства – сканеры безопасности. Используются для анализа уязвимостей и несоответствия в опциях ОС, СУБД, сетевого оборудования. Обнаруженные уязвимости протоколируются и передаются администраторам ИС, сетевым администраторам для уничтожения в установленные сроки.

Подсистема обнаружения проникновений, обязана обеспечивать выявление сетевых атак на составляющие ИС присоединенные к сетками совокупного использования и (или) интернационального обмена.

Перечень возможностей подсистемы реализуется программными и программно-аппаратными средствами, на межсетевых экранах. Администратор сети ведет протоколирование и систематический прогноз доступа, осуществляет контроль содержание трафика, проводит тест лог-файлов.

На межсетевом экране заводится лог-файл, куда записываются все обращения (попытки творения соединений) в сеть и из сети. Лог файл обязан храниться локально и удаленно.

Система обнаружения атак бережёт информацию о атаках и сомнительной активности кроме того в лог-файл.

Тест лог-файлов в форме отчета администратор сети передает работнику ИБ в случае конфликтов глобальных атак, или же по его запросу.

Маршрутизаторы задают систему деятельности безопасности и воспрещают доступ из 1-го сектора сети в другой. Настройкой маршрутизаторов занимается администратор сети.

Локальная безопасность

1. Антивирусная защита.

Антивирусная защита создана для обеспечения антивирусной защиты серверов и АРМ пользователей колледжа.

Средства антивирусной защиты созданы для реализации последующих функций:

1) резидентный антивирусный мониторинг;

2) антивирусное сканирование;

3) скрипт-блокирование;

4) централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администратористрирование, просмотр докладов и статистической информации по работе продукта;

5) автоматизированное обновление антивирусных баз;

6) ограничение прав пользователя на остановку исполняемых задач и конфигурации опций антивирусного программного обеспечения;

7) автоматический пуск незамедлительно после загрузки операционной системы [38, с.182].

Антивирусная защита реализуется методом установки антивирусного программ на всех составляющих ИС. Тест производительности защиты ведется серьезным работником ЦНТ, с применением тестовых компьютеров и контролируется работником ИБ.

Разграничение прав доступа к информационным системам и системам хранения этих.

Для входа в компьютерную сеть работник обязан использовать логин и пароль. Дополнительноускается режим безпарольного (гостевого) доступа к образовательному порталу.

В целях защиты информации организационно и технически делятся подразделения колледжа, имеющие доступ и работающие с разной информацией (в разрезе ее конфиденциальности и смысловой направленности). Эта цель принимается решение с применением полномочий точных ИС, где в целях обеспечения защиты этих доступ и права пользователя ограничивается набором прав и ролей. Права назначаются согласно с производственной потребностью, определяемой администратором ИС.

Все воздействия пользователей ориентируются Регламентом по обеспечению информационной безопасности для пользователей, которую они исследуют при получении доступа к ИС.

Физическая безопасность.

Все объекты опасные с стороны информационной безопасности (все сервера баз данных) находятся в отдельном помещении, доступ в которое разрешен исключительно работникам, имеющими подходящее разрешение и отнесены приказом директора.

Порядок доступа ориентируется Регламентом доступа в серверное помещения.

Обеспечение защиты индивидуальных данных.

Все работники колледжа, являющиеся пользователями ЕМОС, обязаны верно знать и строго исполнять установленные правила и обязонности по доступу к защищаемым объектам и соблюдению принятого режима безопасности индивидуальных данных.

При вступлении в должность нового работника конкретный начальник подразделения, в которое он поступает, должен организовать его ознакомление с должностной аннотацией и нужными документами, регламентирующими требования по охране индивидуальных этих, а еще

изучение умениям исполнения процедур, важных для организованного применения ЕМОС.

Работники колледжа обязаны обеспечить соответствующую защиту оборудования, оставляемого без присмотра, особо в тех случаях, когда в здание имеют доступ чужие лица. Все пользователи обязаны знать требования по безопасности и процедуры защиты оборудования, оставленного без присмотра, а еще собственные обязонности по обеспечению такой защиты.

Работникам воспрещается устанавливать стороннее программное обеспечение, подключать собственные мобильные приспособления и носители информации, и аналогично записывать на них защищаемую информацию [24, с.372].

Работникам запрещается разглашать содержание защищаемой информации, которая стала им доступна при работе с информационными системами колледжа, третьим лицам.

Дублирование, резервирование и хранение информации

Для обеспечения физической целостности этих данных, во избежание умышленного или же неумышленного ликвидирования или преломления защищаемой информации и конфигураций информационных систем организуется резервное копирование баз этих данных, конфигураций, файлов опций, конфигурационных файлов.

3.6. Оценка эффективности мероприятий по совершенствованию информационной безопасности в образовательной организации Учреждение «Костанайский социально-технический колледж»

Эффективность обеспечения информационной безопасности в образовательной организации будет низкой при отсутствии целенаправленных действий по управлению информационными рисками, направленными на причинение ущерба ЕИП образовательной организации.

Для повышения уровня информационной безопасности ЕИП образовательного учреждения необходимо проведение чётко выверенных мероприятий анализа рисков ИБ организации. Ведь ответственный подход к безопасности в образовательной организации – это необходимость в условиях современной информационной действительности. А экономическое обоснование мер предоставит дополнительные возможности, позволяющие избежать непредсказуемых ресурсных затрат образовательному учреждению. Оценка экономических затрат мер совершенствования информационной безопасности колледжа представлена в таблице 1.

Таблица 1

- Оценка экономических затрат по внедрению межсетевого экрана Quantum Spark .

№ п/п	Наименование товаров и услуг	Цена, тенге	Количество	Стоимость, тенге
1.	Программно - аппаратный комплекс Check Point Quantum Spark 1600	3500000	1	3500000
2.	Консультация			бесплатно
3.	Установка и настройка Quantum Spark 1600			бесплатно
Итого:				3500000

Комплексное решение по защите сети:

Тенденция к постоянному росту числа и компетентности кибермошенников, разработка нового и совершенствование существующего зловредного программного обеспечения требует особенного внимания к проектированию и оснащению сетевой инфраструктуры для малого и среднего бизнеса. Check Point является ведущим производителем программно-аппаратных комплексов для защиты от современных угроз. Check Point Threat Prevention одно из них. Программное обеспечение в купе с «железкой» позволяет закрыть следующие задачи:

- межсетевой экран
- IPS
- Антибот
- Антивирусное решение
- Контроль над приложениями
- Сканирование URL
- Эффективная песочница SandBlastTM

Входящее в состав Check Point SandBlast Zero-Day Protection решение Threat Emulation изолирует и обезвреживает подозрительные файлы на стадии входа в инфраструктуру пользователя. Будучи облачным решением, Threat Emulation позволяет сэкономить ресурсы компании, как программно-аппаратные, так и профессиональные. Подозрительные файлы автоматически помещаются в карантин и изучаются в облачной среде.

Программно - аппаратный комплекс Check Point Quantum Spark 1600 надежно защищает корпоративную сеть, при этом являясь интуитивно понятными и не сложными в процессе внедрения и настройки, что приводит к экономию времени и средств. Check Point Quantum Spark 1600 с высокой пропускной способностью и емкостью портов является оптимальным межсетевым экраном нового поколения для больших филиалов и сетей среднего и малого бизнеса.

Программная часть:

Защита: Firewall, VPN, User Awareness, QoS, Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Email Security and SandBlast Threat Emulation (sandboxing)

Unicast, Multicast Routing: OSPFv2, BGPv4 and 4++, RIP, PIM (SM, DM, SSM), IGMP

Мобильный доступ.

Следует отметить, что внедрение Программно – аппаратного комплекса Check Point Quantum Spark 1600 затратно для образовательной организации,

но штрафные санкции, применяемые при выявлении нарушений в области информационной безопасности несоизмеримо выше и применяются не только по отношению к образовательной организации, но и к руководителю, как юридическому лицу, а также подразделению или должностному лицу, допустившему подобные нарушения.

Так выявление нарушений в области информационной безопасности для образовательной организации, грозят ответственностью, предусмотренной статьями закона об административной, гражданской, уголовной, дисциплинарной ответственности, применяемые для организации, руководителя организации - юридического лица, подразделения или виновного работника. Серьёзность последствий определяется законом.

Анализ нормативно-правовых требований согласно законам РК для юридического лица

1. Согласно п. 2 ст. 147 Уголовного кодекса РК, за незаконный сбор сведений о частной жизни лица, которые составляют его личную или семейную тайну, без его согласия при существенном ущербе грозит штраф или исправительные работы до 5000 МРП (18,46 млн тенге), общественные работы до 800 часов, ограничение или лишение свободы на срок до 3 лет.

2. Статья 205 УК РК – неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций, который в зависимости от тяжести последствий предусматривает наказание в виде штрафа в размере до ста шестидесяти месячных расчетных показателей(1 629 120) до двух лет.

3. за нарушение законодательства РК о персональных данных и их защите предусмотрен административный штраф от 10 до 1000 МРП (3 932 000). Также предусмотрена административная ответственность за нарушение Закона и законодательства Республики Казахстан об информатизации (статьи 79 и 641 Кодекса Республики Казахстан «Об административных правонарушениях»), а также уголовная ответственность

за нарушение неприкосновенности частной жизни и Закона (статья 147 Уголовного кодекса Республики Казахстан).

Выводы очевидны: Штрафные санкции только юридического лица превышают затраты на приобретение Check Point Quantum Spark 1600 для информационной безопасности образовательной организации. Тем самым подтверждая выгодность покупки программно - аппаратного комплекса для образовательного учреждения, становясь рентабельно оправданным действием в сложившихся современных условиях.

Тем более, что значительно возросли штрафные санкции и для должностных лиц, и организаций, что немаловажно на сегодняшний момент и определяет дополнительные расходы образовательной организации. Усугубляясь рисками репутационного характера как для организации в целом, так и для её руководителя, и должностных лиц в частности, нанося непоправимый ущерб имиджу таковых. На лицо, серьёзность темы и стимуляция ответственности, в объёме весомого аргумента в пользу совершенствования информационной безопасности единого информационного пространства образовательной организации, посредством внедрения программно - аппаратного комплекса.

ВЫВОДЫ ПО ТРЕТЬЕЙ ГЛАВЕ

В третьей главе нами предложены рекомендации по выбору средств защиты корпоративной информационной системы и приведена экономическая оценка эффективности предложенных средств.

ЗАКЛЮЧЕНИЕ

Представленная работа посвящена теме «Выбор средств защиты корпоративной информационной системы образовательной организации ».

По результатам анализа был раскрыт ряд проблем, имеющих отношение к рассматриваемой теме, и сделаны выводы о необходимости дальнейшего изучения – улучшения состояния вопроса. В персональных компьютерах и в вычислительных сетях колледжа сосредотачивается информация, исключительное пользование которой, принадлежит определенным лицам или группам лиц, действующим в порядке личной инициативы или в соответствии с должностными обязанностями. К тому же в вычислительных сетях принимаются меры по защите вычислительных ресурсов сети от их несанкционированного использования, т.е. доступа к сети лиц, не имеющих на это права. Для этого используют пароли, учетную запись, порядок доступа сотрудников. Физическая защита более надежна. В здании учреждения ведется видеонаблюдение этажей. Разработаны должностные инструкции служащих разграничивающие их права и обязанности, заключены дополнительно соглашения к трудовым договорам сотрудников о неразглашении ими конфиденциальной информации регламентирующие ответственность в области защиты информации, инструкции по эксплуатации системы охранной сигнализации и видеонаблюдения, установлена антивирусная система защиты на рабочие места сотрудников, доступ к рабочим местам сотрудников разграничен паролями. В учреждении существует положения о порядке доступа сотрудников к ресурсам Интернет и правила пользования электронной почты.

Сделав выводы можно сказать о том, что учреждение заботится о сохранности информации, следит за ходом работы сотрудников, бережет свою репутацию. Защита информации в учреждении находится, на должном уровне.

Рассмотрена специфика защиты информации в образовательной системе и предложены рекомендации по улучшению системы защиты информации.

В ходе работы были протестированы основные параметры систем колледжа и определены слабые места. В связи, с чем были разработаны рекомендации по следующим направлениям:

1. Тест опасностей, их источников и рисков. Источниками вероятных опасностей информации являются: компьютеризированные учебные аудитории, в которых наблюдается учебный процесс; Интернет; рабочие станции неквалифицированных в области ИБ сотрудников колледжа.

2. Регламент работы. Для аутентификации пользователей и сотрудников преподавательского персонала, компьютерах в учебных аудиториях вполне возможно использовать ролевое управление доступом (РУД). Сущность технологии - в существе какой-то роли, связывающей пользователя и его привилегии в системе. С ее поддержкою вполне возможно отлично выстроить гибкую систему деятельности разграничения доступа в многопользовательской системе.

3. Барьер защиты от атак снаружи (Интернет) – роутер (Microtik). Вторым рубежом может работать МСЭ: аппаратно-программный компьютерлекс Check Point Quantum Spark 1600.

Предметом защиты информационной безопасности является:

1. Порядок доступа к информационным системам, обрабатывающим конфиденциальную информацию.

2. Работа в сети интернет.

3. Сетевая безопасность.

4. Локальная безопасность.

5. Физическая безопасность (доступ в помещения).

6. Обеспечение защиты индивидуальных данных

7. Дублирование, резервирование и хранение информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Аверченков, В. И. Организационная защита информации [Текст] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – Москва : Флинта, 2015. – 320 с.

2 Алексеев, В. И. Информационная безопасность муниципальных образований [Текст] / В. И. Алексеев. – Воронеж : Изд-во ВГТУ, 2018. – 320 с.

3 Алексеев, В. М. Международные критерии оценки безопасности информационных технологий и их практическое применение [Текст] : учеб. пособие. – Пенза: Изд-во Пенз. гос. ун-та, 2019. – 200 с.

4 Астахов, Л. М. Аудит безопасности информационных систем [Текст] / Л. М. Астахов // Конфидент. – 2015. – № 2. – С.15-23.

5 Бабаш, А. В. Информационная безопасность [Текст] : лабораторный практикум / А. В. Бабаш, Е. К. Баранова, Ю. Н. Мельников. – Москва : КноРус, 2019. – 432 с.

6 Бабаш, А. В. Основы организационного обеспечения информационной безопасности объектов информатизации [Текст] / А. В. Бабаш, С. Н. Семкин и др. – Москва : Гелиос АРВ, 2015. –192 с.

7 Баранова, Е. К. Информационная безопасность и защита информации [Текст] : учеб. пособие / Е. К. Баранова, А. В. Бабаш. – Москва : Риор, 2017. – 476 с.

8 Бармен, С. Разработка правил информационной безопасности [Текст] / С. Бармен. – Москва : Вильямс, 2018. – 208 с.

9 Борисов, М. А. Основы организационно-правовой защиты информации [Текст] / М. А. Борисов, О. А. Романов. – 3-е изд., перераб. и доп. – Москва : ЛЕНАНД, 2014. – 248 с.

10 Будников, С. А. Информационная безопасность автоматизированных систем [Текст] : учеб. пособие / С. А. Будников, Н. В.

Паршин. – 2-е изд. – Воронеж : Издательство им. «Е. А. Болховитинова», 2015. – 340 с.

11 Васильков, А. В. Информационные системы и их безопасность [Текст] : учеб. пособие / А. В. Васильков, А. А. Васильков, И. А. Васильков. – Москва : Форум, 2013. – 528 с.

12 Вигерс, К. Разработка требований к программному обеспечению [Электронный ресурс]. – Режим доступа: http://bulletinsite.net/books/programmer/karl-v/2004/files/razrabtrebovaniy2004.pdf

13 Вержбалович, Д. И. Кибервойна [Текст] : аспекты безопасности использования информационного пространства / Д. И. Вержбалович. – Минск : Беларуская Энцыклапедыя імя Петруся Броўкі, 2015. – 117 с.

14 Вопросы обеспечения информационной безопасности научных, производственных и финансовых структур на базе программно-технических средств [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/8769.html

15 Ворона, В. А. Теоретические основы обеспечения безопасности объектов информатизации [Текст] : учеб. пособие / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. – Москва : Горячая линия, 2016. – 306 с.

16 Галатенко, В. А. Основы информационной безопасности [Текст] : учеб. пособие : для студентов вузов по спец. 351400 «Прикладная информатика» / В. А. Галатенко. – 4-е изд. – Москва : Интернет-Университет Информационных Технологий, 2012. – 205 с.

17 Геннадиева, Е. Г. Теоретические основы информатики и информационная безопасность [Текст] / Е. Г. Геннадиева. – Москва : Радио и связь, 2018. – 320 с.

18 Гринсберг, А. С. Защита информационных ресурсов государственного управления [Текст] / А. С. Гринсберг. – Москва : ЮНИТИ, 2015. – 230 с.

19 Девянин, П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах [Текст] / П. Н. Девянин. – Москва : Радио и связь, 2017. – 176 с.

20 Девянин, П. Н. Информационная безопасность предприятия : учеб. пособие / П. Н. Девянин, А. А. Садердинов, В. А. Трайнев. – Москва : Эксмо, 2016. – 335 с.

21 Девянин, П. Н. Модели безопасности компьютерных систем [Текст] : учеб. пособие для вузов / П. Н. Девянин. – Москва : Академия, 2015. – 144с.

22 Дейтел, Х. М. Операционные системы. Распределенные системы, сети, безопасность / Х. М. Дейтел, П. Д. Дейтел, Д. Р. Чофнес. – Москва : БИНОМ, 2017. – 704 с.

23 Домарев, В. В. Безопасность информационных технологий. Системный подход [Текст] / В. В. Домарев. – Москва : Диасофт, 2018. – 992 с.

24 Запечинков, С. В. Информационная безопасность открытых систем [Текст] / С. В. Запечинков. – Москва : ГЛТ, 2018. – 558 с.

25 Инструкция о порядке предоставления и прекращении компьютерных возможностей пользователей на доступ к ресурсам автоматизированной системы Костанайского регионального центра [Текст]. – Костанай : Энергоинформ, 2017. – 145 с.

26 Информационные технологии [Текст] : учебное пособие / А. А. Вичугова, В. Н. Вичугов, Е. А. Дмитриева, Г. П. Цапко. – Томск : Изд-во ТПУ, 2019. – 105 с.

27 Касперский, К. Записки исследователя компьютерных вирусов [Текст] / К. Касперский. – Москва : Академия, 2016. – 316 с.

28 Каторин, Ю. Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами [Текст] : учеб. пособие / Ю. Ф. Каторин, А. В. Разумовский, А. И. Спивак; под ред. Ю. Ф. Каторина. – Санкт-Петербург : НИУ ИТМО, 2017. – 416 с.

29 Корнипаев, И. Требования для программного обеспечения [Текст] : рекомендации по сбору и документированию / И. Корнипаев. – Москва : Книга по требованию, 2018. – 118 с.

30 Корт, С. Теоретические основы защиты информации [Текст] / С. Корт. – Москва : Гелиос АРВ, 2015. – 230 с.

31 Куприянов, А. И. Основы защиты информации [Текст] : учеб. пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. – 2-е изд. – Москва : Академия, 2017. – 256с.

32 Максимов, Ю. Н. Защита информации в системах и средствах информатизации и связи [Текст] / Ю. Н. Максимов. – Санкт-Петербург : Питер, 2015. – 340 с.

33 Материалы и журналы персонального компьютера [Электронный ресурс]. – Режим доступа: www.computerra.ru

34 Мельников, В. П. Информационная безопасность и защита информации [Текст] / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – Москва : Академия, 2018. – 336 с.

35 Методологии разработки программного обеспечения [Электронный ресурс]. – Режим доступа : http://habrahabr.ru/sandbox/43802

36 Методы и технические средства обеспечения безопасности [Текст] : лабораторный практикум. – Минск : БГУИР, 2015. – 66 с.

37 Организационно-правовое обеспечение информационной безопасности [Текст] : учеб. пособие для студ. учреждений сред. проф. Образования / Е. Б. Белов, В. Н. Пржегорлинский. – Москва : Академия, 2017. – 336 с.

38 Петраков, А. В. Основы практической защиты информации [Текст] : учеб. пособие. – Москва : Академия, 2018. – 281 с.

39 Платонов, В. В. Программно-аппаратные средства защиты информации [Текст] / В. В. Платонов. – Москва : Академия, 2017. – 625 с.

40 Положение о отделе автоматизированных систем диспетчерского управления и вычислительной техники Костанайского регионального центра [Текст]. – Костанай : Энергоинформ, 2017. – 45 с.

41 Прохода, А. Н. Обеспечение интернет-безопасности [Текст] / А. Н. Прохода. – Москва : РГГУ, 2017. – 184 с.

42 Руководство по применению АСКУЭ Костанайского регионального центра «Энергоинформ» [Текст]. – Костанай : Энергоинформ, 2019. – 60 с.

43 Сиротский, А. А. Защита информации и обеспечение безопасности в беспроводных телекоммуникационных сетях [Текст] / А. А. Сиротский // Информационные технологии. Радиоэлектроника. Телекоммуникации : сб. ст. междунар. науч.-техн. конф. – Тольятти, 2012. – Ч. 3. – С. 256-262.

44 Торокин, А. А. Основы инженерно-технической защиты информации [Текст] / А. А. Торокин. – Москва: Академия, 2017. – 345 с.

45 Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] : учеб.пособие для вузов / П. Б.Хорев . – Москва : Академия, 2015. – 256 с.

46 Цирлов, В. Р. Основы информационной безопасности [Текст] : краткий курс / В. Л. Цирлов. – Москва : Феникс, 2018. – 256 с.

47 Чернопятов, А. Наука, образование и практика: профессионально-общественная аккредитация, тьюторство, информационные технологии, информационная безопасность [Текст] / А. Чернопятов. – Москва : Русайнс, 2017. – 144 с.

48 Чефранова, А. О. Система защиты информации ViPNet. Практикум [Текст] : учебно-методическое пособие / А. О. Чефранова, Н. В. Кабакова, Ю. Ф. Алабина. – Москва : Высшая школа, 2015. – 346 с.

49 Шаньгин, В. Ф. Информационная безопасность и защита информации [Текст] / В. Ф. Шаньгин. – Москва : ДМК Пресс, 2017. – 249 с.

50 Щербаков, А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты [Текст] / А. Ю. Щербаков. – Москва : Книжный мир, 2019. – 352 с.

51 Ярочкин, В. И. Технические каналы утечки информации [Текст] / В. И. Ярочкин. – Москва : Академия, 2015. – 350 с.