МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Проект политики информационной безопасности университета»**

Студент:

Николаева Евгения Владимировна

Вариант 11

Преподаватель:

Савельева Маргарита Геннадьевна

Минск 2023

Оглавление

[1.Обоснование актуальности, цели и задачи разработки ПИБ 3](#_Toc127196040)

[2. Объекты защиты. 5](#_Toc127196041)

[2.1Описание структуры организации (учреждения), периметра и внутренней структуры ИВС. 5](#_Toc127196042)

[2.2.Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности. 6](#_Toc127196043)

[3. Основные угрозы и их источники. 8](#_Toc127196044)

[3.1.Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних. 8](#_Toc127196045)

[4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты. 11](#_Toc127196046)

[5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения). Выводы и предложения. 13](#_Toc127196047)

**Цель работы:** приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

# **1.Обоснование актуальности, цели и задачи разработки ПИБ**

**Политика информационной безопасности (ПИБ) организации или учреждения –** совокупность правил, процедур, практических методов, руководящих принципов, документированных управленческих решений, направленных на защиту информации и связанных с ней ресурсов и используемых всеми сотрудниками организации или учреждения в своей деятельности.

Обеспечение ИБ на предприятиях и в учреждениях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость обеспечения ИБ определяется либо высокой степенью автоматизации бизнес-процессов, либо наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерческую, но и государственную тайну, а также другие виды конфиденциальной информации: сведения, составляющие банковскую тайну, различные виды персональных данных, в том числе врачебная тайна, интеллектуальная собственность компаний-партнеров и т. п.

Университеты в век информационных технологий нуждаются в защите своей информации. И с каждым годом, в связи с развитием информационных технологий, всё более разнообразными и сложными становятся угрозы и атаки, способные нанести огромный материальный и моральный ущерб университету, вплоть до его закрытия. Поэтому университет должен обеспечить безопасность персональных данных студентов и рабочих, финансовых данных, а также интеллектуальных данных. Её разглашение или утечка грозит, как минимум, подрывом репутации. Для оптимального решения этой задачи необходимо разработать политику информационной безопасности страховой компании, которой неукоснительно должны следовать все его служащие.

Рост преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Потому на основании этого вы можем выделить цели и задачи:

Цели:

* защита от любой утраты или внесения несанкционированных изменений,
* конфиденциальность, недоступность для третьих лиц,
* доступность в любое время для любого авторизированного пользователя,
* сохранение данных в целостности и неприкосновенности.

Задачи:

* создание нормативно-правовой базы,
* разработка мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения.
* создание концепции информационной безопасности, которая определяет в целом цели политики и основные ее принципы в увязке со статусом, целями и задачами организации или учреждения;
* создание правил и принципов защиты информации;
* описание действий по защите информации при работе с ней;
* создание плана мероприятий по обучению и тестированию сотрудников, имеющих доступ к информационным ресурсам.

Все вышеуказанные элементы должны быть взаимосвязанными и непротиворечивыми. Для эффективной организации системы информационной безопасности целесообразно разработать аварийные планы. Они необходимы на случай восстановления информационных систем при возникновении форс-мажорных обстоятельств: аварий, катастроф и т. д.

# **2. Объекты защиты.**

## **2.1. Описание структуры организации (учреждения), периметра и внутренней структуры ИВС.**

Рассмотрим подробнее внутреннюю структуру универа, её распределение по структурным единицам.

В общем и целом, структура универа состоит из двух сущностей. Первая – это тот, кто учиться. А вторая, естественно, тот, кто преподает/управляет. В роли студентов выступают обычные люди, которым потребовались те или иные знания. В роли преподавателя выступает те, кто закончили университет или те, кто имеют знания в области обучения. Так как мы рассматриваем конкретно информационную безопасность, то можно опустить некоторые элементы работы **университета**, такие как реклама.

Так же стоит отметить такие структурные как:

* Канцелярия — Отдел учреждения, занятый делопроизводство, оформление текущей документации, ведающий служебной перепиской.
* Планово-экономический отдел — Это структурное подразделение предприятия, которое занимается сбором экономических показателей компании, их анализом и разработкой экономических планов.
* Бухгалтерия — отдел, который ведет бухгалтерский учет и составляет текущую и годовую отчетность
* Административно-хозяйственная служба — это подразделение компании, основная задача которого — создание условий для работы сотрудников всей организации.
* Научно-учебный компьютерный центр — это подразделение, которое оснащает студентов необходимой техникой и программами.
* Учебный отдел — основное подразделение, которое оказывает образовательные услуги по отдельным образовательным программам с выдачей документа государственного образца или образца, утверждённого в установленном порядке.
* Ректорат — совещательный и исполнительный орган, обеспечивающий, в том числе, предварительную проработку вопросов, относящихся к компетенции
* Отдел Кадров — отдел, который осуществляет кадровое обеспечение.
* Деканаты факультетов- управляющий орган подразделения ВУЗа (факультета), выполняет руководящую, координирующую и контролирующую функции.
* Заведующие кафедрой — руководитель кафедры в высших учебных заведениях, как правило, профессор, доктор наук.
* Другие сотрудники

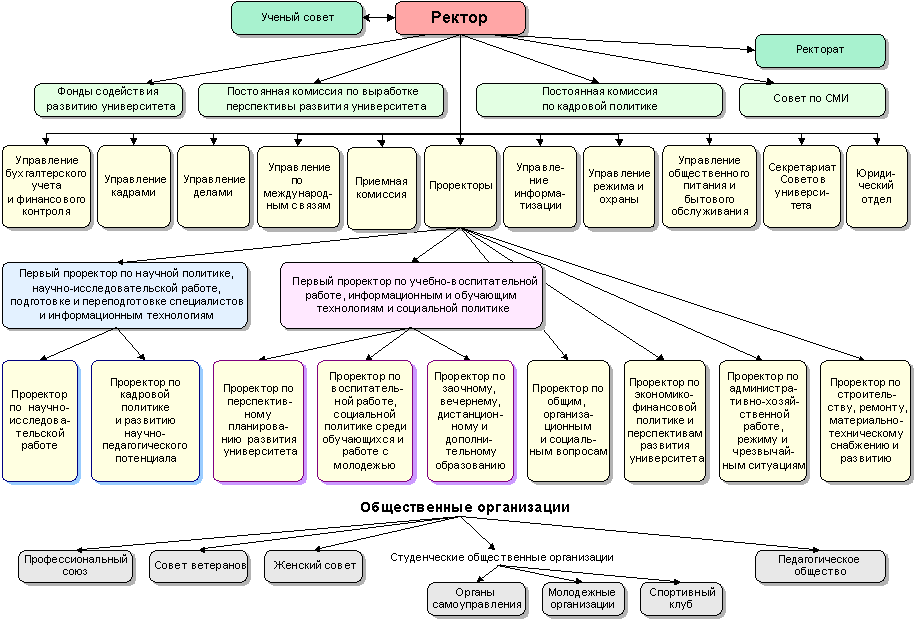


Рисунок 2.1 – Структура универа

## **2.2.Полный обзор всех возможных объектов, а также субъектов информационных отношений, для защиты которых должны быть приняты меры по обеспечению информационной безопасности.**

**Вузы** -это большая инфраструктура, что обладает огромным количеством данных, содержащим различную информацию разного характера, а так же большой человеческий потенциал. Потому все можно разделить на объекты(сама информация) и субъекты(люди, которые взаимодействуют с этой информацией).

Рассмотрим объекты в университете, которые необходимо обеспечить информационной безопасностью:

* структурированная учебная информация (учебные методички, библиотеки, базы данных и др.);
* Серверы, каналы связи, периферийные устройства, различное по;
* Научно-исследовательские работы;
* персональные сведения, касающиеся учащихся и преподавателей;
* информация по финансово-экономической деятельности образовательного учреждения;
* время работников сотрудников;
* другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

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

Если говорить о субъектах, то к ним относятся:

* должностные лица и работники структурных подразделений
* Студенты
* юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются
* Компьютеры
* другие юридические и физические лица, задействованные в процессе создания и функционирования.

# **3. Основные угрозы и их источники.**

## **3.1. Анализ потенциальных угроз: естественных и искусственных, а также преднамеренных и непреднамеренных, внешних и внутренних.**

**Угроза безопасности** - потенциальное нарушение безопасности, любое обстоятельство или событие, которое может явиться причиной нанесения ущерба предприятию в целом.

Все многообразие потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: **естественные (объективные) и искусственные (субъективные)**.

* **Естественные угрозы** – это угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека.
* **Искусственные угрозы –** это угрозы, вызванные деятельностью человека.

Источники угроз по отношению к самой информационной системе могут быть **как внешними, так и внутренними**. Основные источники угроз безопасности информации можно классифицировать следующим образом:

* **непреднамеренные** (ошибочные, случайные, без злого умысла и корыстных целей);
* **преднамеренные** (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п).

Чтобы выделить основные угрозы и их источники стоит отметить, что вуз - публичное заведение с непостоянной аудиторией, т.е каждый год мы имеем достаточно большой поток новых студентов. Потому основную группу потенциальных нарушителей составляют студенты.

Из выше сказанного можно сделать вывод, что особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и сама деятельность подростков, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус. Выделяются четыре группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

* компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;
* программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
* данные, хранимые как на жестких дисках, так и на отдельных носителях;
* сам персонал, отвечающий за работоспособность IT-систем;
* дети, подверженные внешнему агрессивному информационному влиянию и способные создать в школе криминальную ситуацию. В последнее время перечень таких ситуаций существенно расширился, что говорит о возможной целенаправленной психологической атаке на сознание детей и подростков.

Рассмотрим все по порядку. Исходя из вышесказанного определения к **естественным угрозами** мы можем отнести угрозы, не зависящие от намерения персонала, учащихся или третьих лиц, например, любые аварийные ситуации (стихийные бедствия).

Все эти угрозы информационной безопасности носят временный характер, предсказуемы и легко устраняются действиями сотрудников и специальных служб.

Если говорить про **искусственные угрозы,** то они могут иметь разный характер *внешних или внутренний, непреднамеренный или преднамеренный*.

Наименее опасной угрозой являются внутренние непреднамеренные угрозы:

* случайные ошибки персонала, халатность;
* случайные нарушения установленных регламентов;
* не соблюдение техники безопасности.

Их легко обнаружить и устранить, потому универ не понесет больших потерь.

**Намеренные угрозы** информационной безопасности носят более опасный характер и в большинстве случаев не могут быть предвидены. Их виновниками могут оказаться *учащиеся, служащие*(т.е. внутренний характер), *конкуренты, третьи лица*, ранее уволенные сотрудники ,«обиженные» увольнением (внешний харатер) с намерением на совершение кибер-преступления. Для подрыва информационной безопасности такое лицо должно иметь высокую квалификацию в отношении принципов работы компьютерных систем и программ. Наибольшей опасности подвергаются компьютерные сети, компоненты которых расположены отдельно друг от друга в пространстве. Нарушение связи между компонентами системы может привести к полному подрыву ее работоспособности. Важной проблемой может стать нарушение авторских прав, намеренное хищение чужих разработок.

Поговорим о том, что же относится к **преднамеренным угрозам**:

* Спам
* Фарминг
* Кража личных данных отдельного студента/работника, научно-исследовательской работы
* Установка вредоносных ПО
* Физическое воздействие на аппаратуру
* Удаление базы данных студентов/работников
* Несанкционированного доступ
  + **Человеческий**. Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. Кроме того, при наличии доступа к серверу изменения в базы данных могут быть внесены вручную.
  + **Программный**. Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.
  + **Аппаратный.** Он связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

Если говорить про **внутренние дестабилизирующие факторы,** то это:

* ошибки персонала, халатность;
* системные ошибки при постановке задачи проектирования;
* нарушение установленных регламентов;
* не соблюдение техники безопасности;
* Установка вредоносных ПО;
* Программные ошибки в настройке серверов в универе.

**Внешние дестабилизирующие** факторы:

* Неквалифицированные пользователи;
* Внешние климатические условия;
* Электромагнитные и ионизирующие помехи;
* Аварийные ситуации;
* Спам;
* Фарминг.

# **4. Оценка угроз, рисков и уязвимостей. Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты.**

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ. При оценивании рисков учитывается:

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами: количественными, качественными или их комбинацией.

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие некоторой информации принесет ничтожно малый моральный и экономический ущерб универу |
| 1 | Ущерб от атаки есть, но положение и рейтинг универа не затронут |
| 2 | Ущерб от атаки значителен, но не создаёт угрозы для универа, а количество студентов и рабочих изменяется минимально. |
| 3 | Значительные финансовые, интеллектуальные и потери, раскрытие личной информации и потери доверия со стороны студентов, ощутимая часть которых уйдет. |
| 4 | Потери очень значительные. Для восстановления положения потребуются крупные финансовые затраты, есть угроза закрытия универа |
| 5 | Универ прекращает существование |

Таблица 1 — Условная численная шкала для оценки ущерба универа от НСД

Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам представлена в таблице 2

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Практически ежедневно |

Таблица 2 — Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероят  ность | Риск |
| Спам(Mailbombing) | 1 | 0,4 | 0,4 |
| Износ технических средств | 1 | 0,5 | 0,5 |
| Фарминг | 1 | 0,2 | 0,2 |
| Кража личных данных отдельного студента/ работника | 3 | 0,1 | 0,3 |
| Кража научно-исследовательской работы | 1 | 0,1 | 0,2 |
| Удаление базы данных студентов/работников | 1 | 0,1 | 0,1 |
| Ненадежность программ | 3 | 0,1 | 0,3 |
| Установка вредоносных ПО | 2 | 0,3 | 0,6 |
| Попытки проникновения в системы бухгалтерского учета | 2 | 0,1 | 0,2 |
| Программные ошибки в настройке серверов в универе | 2 | 0,2 | 0,4 |
| Захват машинных носителей | 4 | 0,1 | 0,4 |
| Попытки преодоления защиты на физическом уровне(турникеты, сейфы), т.е внутренняя угроза | 2 | 0,3 | 0,6 |
| Попытки преодоления защиты на информационном уровне, т.е внешняя угроза | 3 | 0,2 | 0,6 |
| Копирование защищаемой информации | 3 | 0,1 | 0,3 |
| Итоги: |  |  | 5,1 |

Таблица 3— Оценка рисков

|  |  |
| --- | --- |
| Описание атаки | Меры защиты |
| Спам(Mailbombing) | Давать адрес электронной почты только проверенным источникам;  В качестве преграды для mailbombing-а может выступать и Web-сайт провайдера, иногда настраиваемый таким образом, чтобы он автоматически определял почтовые атаки.  Если количество сообщений из одного источника превышает некие разумные пределы, то все они автоматически поступают в Recycle Bin на сервере. |
| Износ технических средств | Регулярная проверка технического оборудования. Допуск до него только квалифицированных работников. |
| Фарминг | Использовать и регулярно обновлять лицензионное антивирусное программное обеспечение;  Использовать защиту электронного почтового ящика (отключить предварительный просмотр);  Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов. |
| Кража личных данных отдельного студента/ работника | Наличие охраны; Наличие системы видеонаблюдения, использовать и регулярно обновлять лицензионное антивирусное программное обеспечение, использовать шифрование |
| Кража научно-исследовательской работы | Наличие охраны; Наличие системы видеонаблюдения, использовать и регулярно обновлять лицензионное антивирусное программное обеспечение, использовать шифрование |
| Удаление базы данных студентов/работников | Иметь резервные копии на специальных носителях |
| Ненадежность программ | Регулярная проверка ПО. Запрет на пользование «пиратскими» сайтами и файлами.  Иметь хорошее лицензионное антивирусное программное обеспечение. На законодательном уровне запретить скачивание нелицензионного софта. |
| Установка вредоносных ПО | Иметь хорошее лицензионное антивирусное программное обеспечение. |
| Попытки проникновения в системы бухгалтерского учета | Наличие охраны; Наличие системы видеонаблюдения, использовать и регулярно обновлять лицензионное антивирусное программное обеспечение, использовать шифрование. Иметь хорошее лицензионное антивирусное программное обеспечение |
| Программные ошибки в настройке серверов в универе | Допуск до серверов только квалифицированных работников. |
| Захват машинных носителей | Наличие охраны; Наличие системы видеонаблюдения. |
| Попытки преодоления защиты на физическом уровне(турникеты, сейфы), т.е внутренняя угроза | Наличие охраны; Наличие системы видеонаблюдения. Наличие пропускной системы, сейфов. |
| Попытки преодоления защиты на информационном уровне | Наличие хорошей системы шифрования, антивируса. Обучать персонал безопасности в сети и интернете. |
| Копирование защищаемой информации | Наличие хорошей системы шифрования. Заранее объявлять авторское права на информацию. |

Таблица 4— Меры защиты

Таким образом можно сделать вывод, что наиболее опасными видами атаки являются установка вредоносных ПО и несанкционированная установка программ и установка его на рабочие станции, а наиболее частыми атаками является Отказы и неисправности технических средств.

# **5. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов. Описание разработанной политики ИБ и программы обеспечения безопасности на всех уровнях работы организации (учреждения). Выводы и предложения.**

Борьба с различными видами атак на информационную безопасность должна вестись на пяти уровнях:

* правовые (законодательные);
* морально-этические;
* организационные (административные);
* физические;
* технические (аппаратурные и программные).
* Рассмотрим каждый из них.

**Нормативно-правовой способ защиты информационной безопасности**

Защита информации опирается на действующие в этой сфере законы, определяющие отдельные ее массивы как подлежащие защите. Они выделяют те сведения, которые должны быть недоступны третьим лицам по разным причинам (конфиденциальная информация, персональные данные, коммерческая, служебная или профессиональная тайна). Порядок защиты персональных данных определяется в том числе законом «Об информации», Трудовым кодексом. Они и Гражданский кодекс помогают разработать методику для обеспечения защиты сведений, относящихся к коммерческой тайне. Кроме законов необходимо выделить действующие в этой сфере ГОСТы, определяющие порядок защиты данных, и применяемые в этих целях методики и аппаратные средства. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы страховой компании.

**Морально-этические средства обеспечения информационной безопасности**

В образовательной сфере большую роль играет система морально-этических ценностей , которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Морально этические средства состоят из различных стандартов и правил поведения, которые сложились в обществе в процессе развития или были специально разработаны. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т.п.) правил или предписаний.

**Административно-организационные меры**

Этот комплекс мер целиком построен на создании внутренних правил и регламентов, определяющих порядок работы с информацией и ее носителями. Это внутренние методики, посвященные информационной безопасности, должностные инструкции, перечни сведений, не подлежащих передаче. Дополнительно должен быть разработан регламент, определяющий порядок взаимодействия с компетентными органами по запросам о предоставлении им тех или иных данных и документов.

Кроме того, эти методики должны определять порядок доступа к сети Интернет в компьютерных классах, возможность защиты некоторых ресурсов неоднозначного характера от доступа.

**Физические меры**

За данную систему мер и ее внедрение должно отвечать руководство образовательного учреждения и сотрудники IT-подразделений. Перекладывать организацию мер физической защиты компьютерной сети и носителей на сотрудников наемных охранных подразделений недопустимо. Среди физических мер должна быть предусмотрена пропускная система защиты в помещения, содержащие носители информации, организация контроля доступа посетителей, установления различных степеней допуска. Кроме того, к мерам физической защиты может быть отнесено обязательное копирование значимой информации на диски компьютеров, не имеющих доступа к сети Интернет. Обязательно не только установление паролей, но и их регулярная замена.

Комплексную систему защиты всего периметра компьютерной сети должны обеспечивать специализированные программные продукты, например, DLP-системы и SIEM-системы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними. Для тех учебных заведений, бюджет которых не позволяет внедрение профессиональных систем, необходимо использование разрешенных и рекомендуемых программных мер защиты, в частности антивирусов.

Электронная почта, к которой имеют доступ сотрудники и учащиеся, должна быть контролируема. Оптимально также ввести полный запрет на копирование любой информации с жестких дисков компьютеров образовательного учреждения.

**Технические** **меры**

К техническим средствам защиты относятся экранирование помещений для защиты от излучения, проверка поставляемой аппаратуры на соответствие ее спецификациям и отсутствие аппаратных «жучков», средства наружного наблюдения, устройства, блокирующие физический доступ к отдельным блокам компьютера, различные замки и другое оборудование, защищающие помещения, где находятся носители информации, от незаконного проникновения и т.д.

Все меры должны применяться в комплексе, при этом необходимо определение одного или нескольких лиц, отвечающих за реализацию всех аспектов информационной безопасности. Желательно привлечение к этой проблеме родителей учеников, в ряде случаев они помогут провести аудит мер безопасности и порекомендовать современные решения. Кроме того, на родителей должны быть возложены обязанности и по ограничению информации, которую ребенок может получить дома. Необходимо просматривать страницы, посещаемые ребенком. На основании анализа его поиска можно вносить изменения в перечень сайтов, доступ к которым ограничен с компьютеров, установленных в учебном заведении.

**Выводы**

**Политика безопасности** — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На сегодняшний день проблема информационной защиты не является новой. Её появление началось ещё до появления компьютеров. Однако появление и стремительный рост компьютерной техники, а также значимость её в жизни сказалось и на основные принципы построения политики информационной защиты.

Приведенные меры по защите информации являются примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения информационной безопасности для проведения специальных тестов и экспериментов.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки, можем выделить следующие рекомендации, следуя которым возможно снизить риски опасного воздействия и их последствий:

* Общий контроль состояния информационной безопасности Учреждения осуществляется Ректором.
* Текущий контроль соблюдения настоящей Политики осуществляет отдел информатизации и связи спутникового мониторинга транспорта.
* Изменения и дополнения вносятся по инициативе отдела информатизации и или Ректора и утверждаются Ректором.
* Все изменения, внесённые в настоящую Политику информационной безопасности должны учитываться в листе «История изменений» и время от времени проверятся.
* Обучать персонал безопасности в сети и интернете и допуск до серверов только квалифицированных работников.
* Использовать и регулярно обновлять лицензионное антивирусное программное обеспечение;