Учреждение образования “БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ”

Практическая работа №3 «**Разработка политики информационной безопасности бизнес-компании**»

Выполнил:

студентка 2 курса, 5 группы

Буданова Ксения Андреевна

Проверил:

Берников В. О.

Оглавление

[**Введение** 3](#_Toc96696282)

[**Структура средней школы** 5](#_Toc96696283)

[**Оценка рисков** 7](#_Toc96696284)

[**Разработка мер защиты** 8](#_Toc96696285)

[**Вывод** 11](#_Toc96696286)

.

# **Введение**

В век информационных технологий мы имеем выбор хранения информации, таким образом мы можем хранить её:

* На бумажных носителях;
* На различных цифровых носителях.

Каждый день мы используем устройства, из которых мы считываем довольно большие объёмы информации, либо заносим туда свою информацию, которая может быть сугубо личной, либо открытой для всех, так же это относится и к компании. Так что главной задачей для всех является защита своей информации, что является довольно сложной задачей в связи с развитием технологий и появлением глобальной сети. Модели угроз и нарушителей должны быть основным инструментом менеджмента нашей организации при развертывании, поддержании и совершенствовании системы обеспечения информационной безопасности организации.

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации.

Пока не существует формальных методов нейтрализации угроз безопасности информации. По этой причине разработка мер по защите информации должна производиться на основе знаний и опыта соответствующих специалистов (каждый член бригады, выполняющей лабораторную работу, является специалистом-экспертом по защите конфиденциальной информации). Однако в интересах минимизации ошибок процесс разработки должен соответствовать следующим рекомендациям.

Разработку мер защиты информации целесообразно начинать с угроз, имеющих максимальное значение; далее - с меньшей угрозой, и так далее до тех пор, пока не будут исчерпаны выделенные ресурсы. Такой подход гарантирует, что даже при малых ресурсах хватит ресурсов для предотвращения наиболее значимых угроз. Для каждой угрозы разрабатываются меры (способы и средства) по защите информации.

Существуют различные подходы к оценке рисков. Выбор под хода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Разработанная и утвержденная документация должна включать в себя следующие разделы:

- перечисление объектов, в отношении которых устанавливается режим информационной безопасности, их ранжирование по значимости и требуемой степени защиты;

- описания технологий, применяемых для обеспечения сохранности информации;

- перечень действующих и потенциальных угроз информационной безопасности, описание степени их серьезности и реализуемости;

- описание внешних и внутренних субъектов, которые могут стать источниками потенциальной угрозы;

- описание понятия инцидента информационной безопасности, процедур уведомления о его возникновении;

- описание применяемых организационных мер, действий сотрудников компании по обеспечению информационной безопасности;

- описание выбранной политики защиты от вирусных атак, программ-вредителей, возможных действий хакеров;

- описание системы резервного копирования важных данных, ее периодичности, моделей хранения – на дисках, на посторонних серверах;

- описание того, в каком порядке будут проводиться аварийные и восстановительные работы при повреждении аппаратной части в случае пожара, проблем с электросвязью или по иным причинам, повлекшим за собой гибель компьютеров, носителей информации или самих баз данных;

- план мероприятий по постоянному поддержанию готовности системы к работе, ее обновлению при изменении правил сертификации или степени значимости угроз.

Целью политики является регламентирование единых подходов и требований по обеспечению информационной безопасности сотрудниками банка, а также государственными органами и организациями, иными юридическими лицами и индивидуальными предпринимателями в рамках оказания им услуг банком.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

- антропогенные,

- техногенные,

- естественные (природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

- сотрудники организации;

- программное обеспечение;

- аппаратные средства.

К информационным угрозам относятся:

- несанкционированный доступ к информационным ресурсам;

- незаконное копирование данных в информационных системах;

- противозаконный сбор и использование информации;

- использование информационного оружия.

К программным угрозам относятся:

- использование ошибок и «дыр» в ПО;

- компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

- уничтожение или разрушение средств обработки информации и связи;

# **Структура средней школы**

Структура школы состоит из двух сущностей. Первая – это тот, кто учиться. А вторая, естественно, тот, кто преподает. В роли учеников 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 **средней школы**, такие как реклама.

**Средняя школа** — учреждение, предоставляющее образовательные услуги [средней ступени](https://ru.wikipedia.org/wiki/%D0%A1%D1%80%D0%B5%D0%B4%D0%BD%D0%B5%D0%B5_%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), промежуточное звено между [начальной школой](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0%D1%8F_%D1%88%D0%BA%D0%BE%D0%BB%D0%B0) и [старшей школой](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D1%82%D0%B0%D1%80%D1%88%D0%B0%D1%8F_%D1%88%D0%BA%D0%BE%D0%BB%D0%B0&action=edit&redlink=1). В некоторых [странах](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D1%80%D0%B0%D0%BD%D0%B0) [образование](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), полученное в средней школе, считается [начальным](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D1%80%D0%B0%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5).



Рисунок 1 – Структура средней школы

Внимание стоит сконцентрировать на самой работе школы в интернет-пространстве, обратной связи и конкретно на том, что непосредственно зависит от информационных технологий. Но и остальные сотрудники, которые хоть каким-то образом связаны со средней школы в интернете, должны быть проинформированы о информационной безопасности, в целях предотвращения угроз.

# **Оценка рисков**

Перед тем как разрабатывать защиту, сначала нужно понять от чего защищаться. Как я говорил ранее стоит обратить внимание на те элементы средней школы, которые непосредственно находятся в интернете.

Так как нужно идти от большей проблемы к меньшей, то стоит начать с самой страницы . Не редко страницы в интернете подвергаются DDOS атакам. Также, как и в обычной жизни в интернете существует огромное количество спекулянтов и прочих людей, которые ищут лазейки в сайтах, для сбоя работы и получения выгоды.

Чтобы сайт был, его нужно сначала создать. возникает еще одна проблема. Чтобы сайт работал корректно нужен специалист. Уже на этом этапе, этапе разработки сайта, можно устранить некоторые угрозы, которые могут привести к еще большим затратам в будущем.

Также стоит помнить, что при разработке сайта, нужно сделать «userfriendly» интерфейс. Спрятать все элементы, которые могут нанести вред системе.

При разработке back-end части страницы, стоит уделить особенное внимание авторизации пользователей. Выдавать им права пользователя безошибочно. Чтобы права администратора были только у разработчиков.

Выбор не ответственных или малознакомых разработчиков тоже может повлиять на работу сайта после его создания. Человек с нарушенными моральными нормами, может специально сделать «дыру» в программе, для личного пользования уязвимостью.

Также стоит обратить внимание на обратную связь. Нередко люди, которые хотят поступить, хотят узнать больше. Это нормальная практика в современном мире.

# **Разработка мер защиты**

Далее я предложу несколько решений для решения проблем, описанных выше.

Начиная с самого главного, с разработки сайта, вам стоить ответственно подойти к выбору человека, который будет заниматься разработкой. Не стоит искать дешевых специалистов. Лучше переплатить и знать, что с массой возможных проблем вы уже справились. Квалифицированный специалист с опытом на этапе разработке уже устранит «дыры» в ПО. Также стоит провести ручные и автоматические тесты вашей средней школы. Это поможет устранить остальные проблемы перед его запуском.

Чтобы страница работала корректно, его нужно поместить на хороший хостинг. Если вы приобрели собственный сервер, нужно позаботиться о его правильном хранении и работе. Стоит учитывать физические особенности. Например, перебои с электричеством. Для этого стоит установить бесперебойные системы, которые в случае отключения электричества смогу обеспечивать ваш сервер энергией какое-то время, пока поломка не будет устранена или вы не найдете другого решения. Как я писал ранее сайты могут быть подвержены DDOS атакам. Для этого вам и нужен хороший сервер. Сервер с малой пропускной способность быстро выйдет из строя при большой загруженности сайта. Стоит разработать протоколы, которые смогут обеспечить безопасность, при атаках или, когда на сайт зайдет большое количество людей (например, при распродаже).

Все такие не стоит забывать и не информационной стороне вашего сайта. Стоит обучить сотрудников, которые имеют непосредственный доступ к вашему сайту на правах администратора, хотя бы, базовым аспектам информационной безопасности.

Людей, которые занимаются рекламой, тоже стоит проинформировать о безопасности. Так как это средняя школа, то большая часть рекламы будет находиться в интернете. Не стоит размещать рекламу на не проверенных и подозрительных сайтах.

Чтобы не допустить распространения конфиденциальной информации в законодательстве РБ существуют законы по предотвращению данных проблем.

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

- установление особого режима конфиденциальности;

- ограничение доступа к конфиденциальной информации;

- использование организационных мер и технических средств защиты информации;

- осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

- организацию охраны помещений, в которых содержатся носители конфиденциальной информации;

- установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;

- установление пропускного режима в помещения, содержащие носители конфиденциальной информации;

- закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;

- установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);

- организацию ремонта технических средств обработки конфиденциальной информации;

- организацию контроля за установленным порядком.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

- средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;

- средства, обеспечивающие защиту информации при передаче ее по каналам связи;

- средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;

- средства, обеспечивающие защиту от воздействия программ-вирусов;

- материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

# **Вывод**

Вся ответственность по разработке информационной безопасности лежит на вас. Конечно, самому разрабатывать вам ее не придется, но никогда не стоит о ней забывать. Стоит изучить некоторые документы, обратиться за помощью к специалистам.

Важно помнить, что прежде, чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

Опыт показывает, что для достижения удачных решений по защите информации компаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.