МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий

Кафедра Информационных системы и технологии

Специальность 1-40 01 01 «Программное обеспечение информационных технологий»

Специализация Программирование интернет-приложений

**РАЗРАБОТКА ПОЛИТИКИ**

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Национальной академии наук Беларуси**

Выполнил студент Гордеев Игорь Валерьевич

(Ф.И.О.)

Преподаватель \_\_\_\_ассистент Блинова Евгения Александровна

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2018

**ОГЛАВЛЕНИЕ**

|  |  |
| --- | --- |
| Введение............................................................................................................. | 3 |
| 1. Описание структуры академии наук........................................... | 4 |
| 1. Общие положения.............................................................................. | 8 |
| 1. Оценка рисков.................................................................................... | 9 |
| 1. Разработка мер защиты..................................................................... | 10 |
| Вывод............................................................................................................... | 11 |

**ВВЕДЕНИЕ**

**Цель работы** - разработать проект политики информационной безопасности бизнес-компании.

Развитие и рост предприятий очень тесно связан с ростом ИТ-инфраструктуры и информационных систем, сложность и масштабы которых постоянно растут, порождая при этом новые виды угроз, уязвимостей и рисков, которые прямым образом влияют на деятельность организации.

Возникновение проблем в информационной безопасности организации приводит как к финансовым, так и к репутационным потерям. Важная задача руководства – предотвратить эти угрозы, минимизировать риски и обеспечить должный уровень безопасности ИТ-инфраструктуры предприятия.

Основой мер административного уровня, то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Любая защитная мера есть компромисс между снижением рисков и удобством работы пользователя. Таким образом, политика выполняет две основные функции:

* определяет безопасность внутри организации;
* определяет место каждого служащего в системе безопасности.

**ГЛАВА 1. ОПИСАНИЕ СТРУКТУРЫ БИЗНЕС-КОМПАНИИ**

В НАН существует иерархическая структура управления, в которой выделяется 5 уровней управления. Структура академии представлена на рис. 1.1.



Рисунок 1.1 Структура учебного заведения

**Структурные подразделения аппарата управления НАН РБ**

Аппарат Национальной академии наук Беларуси является подразделением Академии наук, осуществляющим организационно-распорядительную работу по обеспечению реализации органами управления Академии наук ее функций. В соответствии с Законом Республики Беларусь О Национальной академии наук Беларуси и Уставом Национальной академии наук Беларуси аппарат Академии наук состоит из структурных подразделений, созданных для подготовки и организации исполнения решений Председателя Президиума НАН Беларуси и органов управления Академии наук, подчиняется Председателю Президиума Академии наук.

В целях обеспечения реализации Академией наук функций высшей государственной научной организации Республики Беларусь, а также отдельных функций республиканского органа государственного управления на аппарат Академии наук возложены следующие основные задачи:

организация выполнения и участие в выполнении декретов, указов и распоряжений Президента Республики Беларусь, решений Правительства Республики Беларусь, иных правовых актов по вопросам научной деятельности, постановлений Общего собрания, Президиума, Бюро Президиума Академии наук, приказов, распоряжений и поручений Председателя Президиума Академии наук, а также осуществление постоянного контроля хода их выполнения;

оперативная и качественная подготовка проектов документов Председателя Президиума Академии наук и органов управления Академии наук;

систематический анализ состояния отдельных вопросов деятельности Академии наук, выявление актуальных проблем и подготовка на этой основе соответствующих предложений;

материально-техническое и организационное обеспечение деятельности органов управления Академии наук, а также мероприятий, проводимых ими.

Аппарат НАН Беларуси оказывает методическую, информационную, консультативную, организационную и иную помощь организациям Академии наук в обеспечении их деятельности, осуществляет иные меры, способствующие повышению эффективности деятельности Академии наук. В настоящее время он состоит из управлений и отделов, возглавляемых руководителями; аппаратов отделений Академии наук, возглавляемых академиками-секретарями отделений Академии наук; почетного президента Академии наук, советников и консультантов Президиума Академии наук, выполняющих поручения Председателя Президиума Академии наук и Президиума Академии наук.

 Деятельность Национальной академии наук Беларуси осуществляется на основе сочетания единоначалия и коллегиальности рассмотрения и решения вопросов органами управления Академии наук с персональной ответственностью их членов за проведение в жизнь принятых решений и состояние дел на порученных участках работы. Органами управления НАН Беларуси являются Общее собрание Академии наук, Президиум Академии наук и Бюро Президиума Академии наук.

Высший коллегиальный орган управления Академии наук -- Общее собрание Академии наук, членами которого являются: Председатель Президиума Академии наук; члены Президиума Академии наук; академики и члены-корреспонденты; руководители научных организаций, находящихся в ведении Академии наук; представители научных организаций, находящихся в ведении Академии наук, избираемые учеными (научно-техническими) советами данных организаций тайным голосованием сроком на 5 лет с правом отзыва и замены, а также представители научных организаций министерств, других республиканских органов государственного управления, учреждений, обеспечивающих получение высшего образования (до 20% членов Общего собрания), избираемые тайным голосованием учеными (научно-техническими) советами указанных организаций Республики Беларусь сроком на 5 лет с правом отзыва и замены.

Общее собрание Академии наук, сессии которого созываются Президиумом НАН Беларуси два раза в год, рассматривает вопросы развития науки и научно-технического прогресса, приоритетные направления фундаментальных и прикладных научных исследований и разработок в Республике Беларусь, утверждает концепции и долгосрочные прогнозы развития науки, принимает решения по вопросам организации и координации фундаментальных и прикладных научных исследований и разработок, избирает в установленном порядке членов Академии наук; принимает в пределах своей компетенции постановления Академии наук, решения об образовании, реорганизации и упразднении отделений наук и региональных филиалов Академии наук, утверждает ежегодные отчеты о деятельности Академии наук, Регламент Общего собрания НАН Беларуси, положения об отделении НАН Беларуси и о выборах членов НАН Беларуси, принимает Устав Национальной академии наук Беларуси, а также изменения и дополнения к нему для последующего внесения в установленном порядке на утверждение Президента Республики Беларусь.

Решения Общего собрания НАН Беларуси обязательны для выполнения Президиумом и Бюро Президиума Академии наук, Председателем Президиума Академии наук, научными организациями и иными юридическими лицами, находящимися в ведении Академии наук, а по вопросам организации и координации фундаментальных и прикладных научных исследований и разработок -- всеми субъектами научной деятельности Республики Беларусь.

**ГЛАВА 2. ОБЩИЕ ПОЛОЖЕНИЯ**

Целью политики НАН РБ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защита прав на неприкосновенность частной жизни, личную и семейную тайну, неукоснительное соблюдение требований законодательства в области персональных данных.

Национальная академия наук Беларуси, торжественно открытая 1 января 1929 года, основана на базе Института белорусской культуры (Инбелкульт, 1922--1928), который был реорганизован в Академию наук в соответствии с постановлением Центрального Исполнительного Комитета и Совета Народных Комиссаров Белорусской ССР от 13 октября 1928 года. За прошедшие 85 лет Академия наук внесла важный вклад в развитие науки и техники в Беларуси, укрепление национальной экономики и обороны, подготовку большого числа специалистов для научно-исследовательских центров, высших учебных заведений и различных отраслей промышленности.

Главный корпус Академии наук (здание Президиума НАН Беларуси), который имеет статус историко-культурной ценности Республики Беларусь, и основная часть ее научно-исследовательских институтов находятся в Минске -- столице Республики Беларусь. Ряд организаций Академии наук расположены в областных центрах республики -- Бресте, Гомеле, Гродно, Могилёве и Витебске, а также в других регионах страны. В целях организации, проведения и координации фундаментальных и прикладных научных исследований и разработок в пределах региона создан Гомельский филиал Национальной академии наук Беларуси.

**ГЛАВА 3. ОЦЕНКА РИСКОВ**

Оценка рисков занимает центральное место в системе управления информационной безопасностью.



Рисунок 1.2. Роль процесса оценки рисков в структуре процессов информационной безопасности

Под риском понимается неопределенность, предполагающая возможность ущерба, связанного с нарушением ИБ. Оценка рисков – это процесс, охватывающий идентификацию риска, анализ риска и сравнительную оценку риска.

  Оценка рисков является эффективным механизмом управления информационной безопасностью в компании, позволяющим:

* идентифицировать и оценить существующие информационные активы компании;
* оценить необходимость внедрения средств защиты информации;
* оценить эффективность уже внедренных средств защиты информации.

Объектами защиты с точки зрения информационной безопасности в управлении являются:

* персональные данные;
* денежные средства;

Политика информационной безопасности почты направлена на защиту информационных ресурсов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников предприятия, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Наибольшими возможностями для нанесения ущерба обладает собственный персонал НАН. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

Существуют четыре действия, производимые с информацией, которые могут содержать в себе угрозу: сбор, модификация, утечка и уничтожение.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

Источниками внутренних угроз являются:

* сотрудники;
* программное обеспечение;
* аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах:

* ошибки пользователей и системных администраторов;
* нарушения сотрудниками академии установленных регламентов сбора, обработки, передачи и уничтожения информации; ошибки в работе программного обеспечения; отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:

* компьютерные вирусы и вредоносные программы;
* организации и отдельные лица;
* стихийные бедствия.

Формами проявления внешних угроз являются:

* заражение компьютеров вирусами или вредоносными программами; несанкционированный доступ (НСД) к корпоративной информации;
* информационный мониторинг со стороны конкурирующих структур, разведывательных и специальных служб;
* действия государственных структур и служб, сопровождающиеся сбором, модификацией, изъятием и уничтожением информации; аварии, пожары, техногенные катастрофы.

По степени преднамеренности проявления **случайные** и **преднамеренные**:

* случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия, ошибки пользователей и т.п.);
* преднамеренные (умышленные действия, например, шпионаж, диверсия, перехват информации, хакерские атаки, фальсификация документов и т.п.).

По размерам наносимого ущерба:

* общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);
* локальные (причинение вреда отдельным частям объекта безопасности);
* частные (причинение вреда отдельным свойствам элементов объекта безопасности).

По степени воздействия на информационную систему:

* пассивные (структура и содержание системы не изменяются);
* активные (структура и содержание системы подвергается изменениям).

По аспекту информационной безопасности, на который направлены угрозы:

* угрозы [конфиденциальности](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D0%B8%D0%B4%D0%B5%D0%BD%D1%86%D0%B8%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C) (неправомерный доступ к информации);
* угрозы [целостности](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BB%D0%BE%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (неправомерное изменение данных);
* угрозы [доступности](https://ru.wikipedia.org/wiki/%D0%94%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%B8) (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы);

**ГЛАВА 4. РАЗРАБОТКА МЕР ЗАЩИТЫ**

**Меры защиты -**  четыре уровня защиты:

**Предотвращение** - только авторизованный персонал имеет доступ к информации и технологии

**Обнаружение** - обеспечивается раннее обнаружение преступлений и злоупотреблений, даже если механизмы защиты были обойдены

**Ограничение** - уменьшается размер потерь, если преступление все-таки произошло несмотря на меры по его предотвращению и обнаружению.

**Восстановление** - обеспечивается эффективное восстановление информации при наличии документированных и проверенных планов по восстановлению.

Сегодня контроль за информацией стал обязанностью каждого пользователя. Контроль за информацией требует новых знаний и навыков для группы служащих. Хороший контроль за информацией требует понимания возможностей совершения компьютерных преступлений и злоупотреблений, чтобы можно было в дальнейшем предпринять контрмеры против них.

Компьютерные терминалы и настольные компьютеры используются везде. Компьютерное оборудование стало дружественным к пользователю, поэтому много людей могут быстро и легко научиться тому, как его использовать.

Число служащих в организации, имеющих доступ к компьютерному оборудованию и информационной технологии, постоянно растет. Доступ к информации больше не ограничивается только узким кругом лиц из верхнего руководства организации. Этот процесс привел к тому, что произошла "демократизация преступления". Чем больше людей получало доступ к информационной технологии и компьютерному оборудованию, тем больше возникало возможностей для совершения компьютерных преступлений.

**Требования по информационной безопасности:**

* все работы в пределах НАН должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию;
* все данные (конфиденциальные или строго конфиденциальные), составляющие тайну НАН и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы;
* руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам;
* в целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля;
* пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким;
* в процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут;
* доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности;
* сотрудникам НАН разрешается использовать сеть Интернет только в служебных целях;
* запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
* работа сотрудников НАН с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации НАН в сеть Интернет;
* сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем НАН;
* сотрудники НАН перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
* запрещен доступ в Интернет через сеть НАН для всех лиц, не являющихся сотрудниками НАН, включая членов семьи сотрудников.
* администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях;
* сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация НАН;
* сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор ЛВС;
* все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для СD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное НАН, является ее собственностью и предназначено для использования исключительно в производственных целях;
* каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности;
* все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к администратору. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных;
* при записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации;
* порты передачи данных, в том числе CD дисководы в стационарных компьютерах сотрудников НАН блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.
* все программное обеспечение, установленное на предоставленном школой компьютерном оборудовании, является собственностью НАН и должно использоваться исключительно в производственных целях;
* cотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника и председателю президиума НАН;
* электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию школы по электронной почте без использования систем шифрования. Строго конфиденциальная информация НАН, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте;
* использование сотрудниками НАН публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования;
* cотрудники НАН для обмена документами должны использовать только свой официальный адрес электронной почты;
* все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.
* в случае кражи переносного компьютера следует незамедлительно сообщить администратору и/или вышестоящему руководителю НАН.
* если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан проинформировать администратора;
* перечень помещений с техническими средствами информационной безопасности утверждается председателем президиума НАН.
* участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с администратором.

**Обеспечение безопасности персональных данных:**

* использование ключ-карт;
* надежное шифрование всех научных разработок;
* возможность получения патента или авторского права;
* использование новейших средств защиты информации;
* доступ к разработкам только доверенным лицам;

**Вывод**

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.

Стратегия обеспечения информационной безопасности школы заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников школы.

Эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети.

Большинство средств защиты при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Лучшая защита от нападения — это не допустить его. Обучение пользователей правилам сетевой безопасности может предотвратить нападения. Защита информации включает в себя кроме технических мер еще и обучение или правильный подбор обслуживающего персонала. Защита информации не ограничивается техническими методами. Основной недостаток защиты — люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети.

**Список литературы**

1. Бракович А.И. доцент, к.т.н.: Конспект лекций
2. Закон Республики Беларусь от 10 ноября 2008 г. № 455-3 «Об информации, информатизации и защите информации».
3. Указ № 515 Президента Республики Беларусь от 30 сентября 2010 г. «О некоторых мерах по развитию сети передачи данных в Республике Беларусь».