МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ   
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных технологий

Кафедра Информационных систем и технологий

Специальность 1—98 01 03 «Программное обеспечение информационной

безопасности мобильных систем»

**ОТЧЕТ ПО ПРАКТИЧЕСКИМ ЗАНЯТИЯМ**

по дисциплине «Основы информационной безопасности»

вариант 10

**Исполнитель**

студент(ка) 2 курса \_7\_ группы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Банкузов Михаил

подпись, дата

**Руководитель**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ржеутская Н. В.

должность, ученая степень, ученое звание подпись, дата

**Практическое задание № 2**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Введение**

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.

Определение политики ИБ должно сводиться к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

• управление доступом к средствам вычислительной техники, программа и данным;

• антивирусную защиту;

• вопросы резервного копирования;

• проведение ремонтных и восстановительных работ;

• информирование об инцидентах об области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Описание границ системы, для которой должен быть обеспечен режим информационной безопасности, рекомендуется выполнять по следующему плану.

1. Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой или модернизации автоматизированной системы обработки информации.

2. Размещение средств вычислительной техники и поддерживающей инфраструктуры. Модель иерархии средств вычислительной техники.

3. Ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы следующих классов: средства вычислительной техники, данные, системное и прикладное программное обеспечение. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методология оценок по этим критериям.

4. Технология обработки информации и решаемые задачи. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

В результате должен быть составлен документ, в котором:

• зафиксированы границы и структура системы;

• перечислены ресурсы, подлежащие защите;

• дана система критериев для оценки их ценности.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

В случае, когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму информационной безопасности является недостаточным. Для того, чтобы сформулировать дополнительные требования, необходимо:

• определить ценность ресурсов;

• к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

• оценить вероятности угроз;

• определить уровень уязвимости ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

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.

Процесс оценивая рисков содержит несколько этапов.

1. Идентификация ресурса и оценивание его количественных показателей (определение негативного воздействия).

2. Оценивание угроз.

3. Оценивание уязвимостей.

4. Оценивание существующих и предполагаемых средств обеспечения.

5. Оценивание рисков.

На основании оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

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 (например, стоимостные);

• качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);

• их комбинацией.

Для того, чтобы конкретизировать определение вероятности в течение которого предполагается защитить ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

• привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

• возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

• технические возможности угрозы, используемые при умышленном воздействии со стороны человека;

• вероятность того, что угроза реализуется;

• степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно техническом уровнях уровне.

К **процедурному уровню** относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

• управление персоналом;

• физическая защита;

• поддержание работоспособности;

• реагирование на нарушения режима безопасности;

• планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности существовать квалификационные требования по ИБ. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д.

Планирование восстановительных работ предполагает:

• слаженность действий персонала во время и после аварии;

• наличие заранее подготовленных резервных производственных площадок;

• официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;

• -схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время, осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой **программно-технического уровня** являются следующие механизмы безопасности:

• идентификация и аутентификация пользователей;

• управление доступом;

• протоколирование и аудит;

• криптография;

• экранирование;

• обеспечение высокой доступности и т.д.

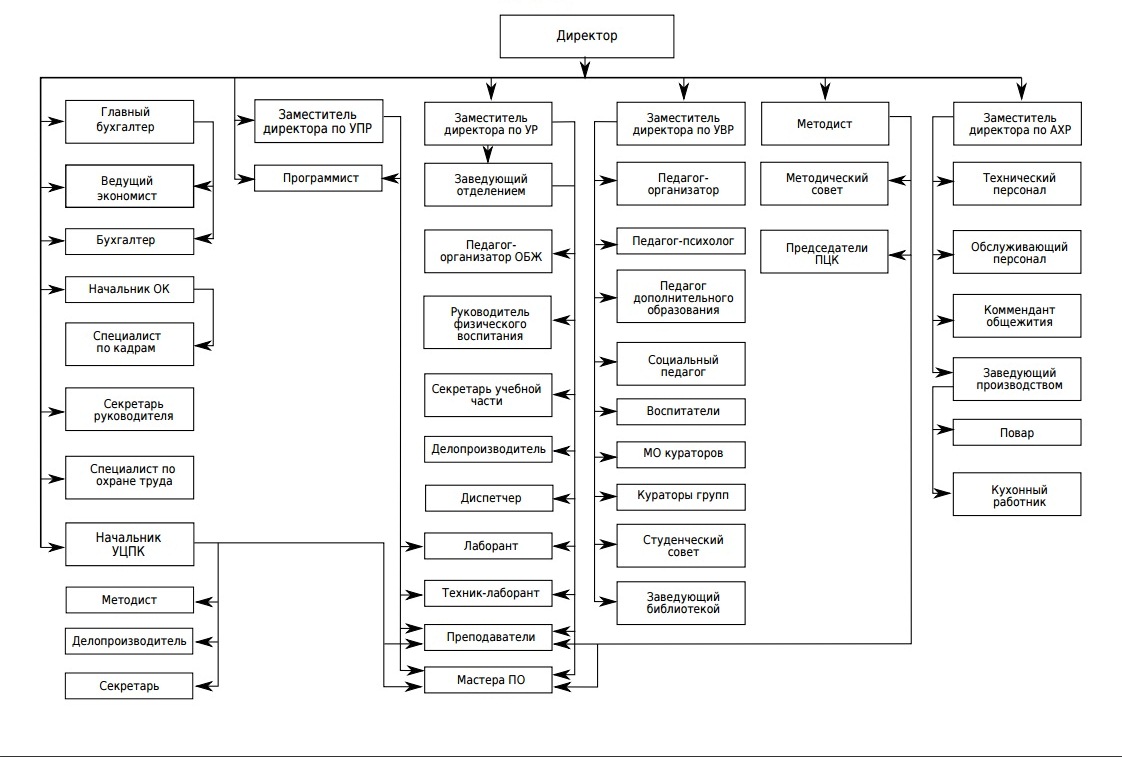
Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивым к сетевым угрозам, учитывать специфику отдельных сервисов.

**Условие задания**

|  |  |
| --- | --- |
| 2. | Техникум |

**Структура техникума:**

1. Административное руководство: Включает директора или ректора техникума, который отвечает за общее управление учебным заведением. Рядом с ним могут быть заместители директора, административный персонал и другие административные должности, отвечающие за различные аспекты работы техникума.
2. Учебный совет: Это орган, состоящий из представителей администрации, преподавателей и студентов, который принимает решения по вопросам образования, учебного плана, кадрового обеспечения и другим важным аспектам обучения.
3. Кафедры и преподаватели: Техникум включает различные кафедры или отделения, каждое из которых специализируется в определенной области знаний или профессиональной области. Каждая кафедра имеет своего руководителя и преподавателей, которые осуществляют обучение студентов в соответствующих дисциплинах.
4. Учебные группы и студенты: Студенты техникума организуются в учебные группы, которые состоят из студентов, обучающихся вместе по определенной специальности или курсу. Каждая группа может иметь своего классного руководителя или наставника, который следит за успеваемостью и общим благополучием студентов.
5. Учебные и лабораторные помещения: Техникум обычно обладает различными учебными и лабораторными помещениями, где студенты получают практические навыки и проводят лабораторные работы в соответствующих областях знаний. Это могут быть аудитории, компьютерные классы, специализированные лаборатории и т. д.
6. Библиотека: Техникум обычно имеет библиотеку, где студенты и преподаватели могут получить доступ к необходимой учебной литературе, научным журналам и другим информационным ресурсам.
7. Административно-хозяйственный отдел: Включает различные службы, отвечающие за финансовое управление, кадровое делопроизводство, материально-техническое обеспечение, организацию питания студентов и другие аспекты, связанные с обеспечением нормального функционирования техникума.



**Оценка рисков для техникума может быть выполнена следующим образом:**

1. Идентификация ресурсов и оценка их количественных показателей:

* Системы вычислительной техники (количество компьютеров, серверов и других устройств).
* Данные (личная информация студентов, учетные записи, академические записи и т.д.).
* Программное обеспечение (системы управления учебным процессом, электронные ресурсы и т.д.).

1. Оценка угроз:

* Несанкционированный доступ к системам и данным (хакерские атаки, утечка паролей).
* Вирусы и вредоносное ПО (заражение компьютеров через вредоносные программы).
* Физические повреждения оборудования (пожар, наводнение, кража).

1. Оценка уязвимостей:

* Недостаточная защита сетевых соединений и устройств.
* Недостаточное обновление и поддержка программного обеспечения.
* Недостаточная обученность персонала по вопросам информационной безопасности.

1. Оценка существующих и предполагаемых средств обеспечения:

* Наличие антивирусной защиты и системы мониторинга сетевой активности.
* Регулярное резервное копирование данных.
* Политика управления доступом и парольная защита.

1. Оценка рисков:

* Вероятность нарушения информационной безопасности (высокая, средняя, низкая).
* Потенциальные последствия нарушений (утечка конфиденциальных данных, нарушение учебного процесса).

**На основе проведенной оценки рисков могут быть предприняты следующие меры для обеспечения информационной безопасности в техникуме**:

* Разработка и внедрение политики информационной безопасности, которая определит стратегию и меры защиты.
* Разработка и внедрение политики управления доступом, которая определит права доступа к информационным ресурсам в зависимости от должностных обязанностей и необходимости.
* Установка и обновление антивирусного программного обеспечения на всех компьютерах и серверах.
* Регулярное резервное копирование данных и их хранение на защищенных носителях.
* Обеспечение физической безопасности помещений, где находится вычислительная техника.
* Установка мощных паролей и регулярное их изменение.
* Мониторинг сетевой активности с целью выявления подозрительных действий или атак.
* Включать проверку сертификатов безопасности, заключение соответствующих соглашений о защите информации и мониторинг деятельности поставщиков и контрагентов.

**Также необходимо разработать административные меры защиты:**

* Разработка и внедрение политики информационной безопасности: Важно разработать документ, который определит стратегию и меры защиты информации в техникуме. Политика должна включать правила использования информационных систем, управление доступом, защиту конфиденциальных данных и другие важные аспекты безопасности.
* Установка ответственности: Необходимо определить ответственных лиц, которые будут отвечать за реализацию политики информационной безопасности и координацию мер по ее соблюдению. Это может быть комитет по информационной безопасности или назначенные сотрудники, которые будут отвечать за обеспечение безопасности информационных систем.
* Обучение и осведомленность: Регулярное обучение сотрудников, преподавателей и студентов основам информационной безопасности и правилам использования информационных систем является важным аспектом. Данные обучающие программы должны включать в себя обучение по защите паролей, распознаванию фишинговых атак, безопасному обращению с электронной почтой и другим аспектам безопасности.
* Управление доступом: Необходимо регулировать доступ к информационным системам и ресурсам на основе принципа "необходимости доступа". Это означает, что каждый пользователь должен иметь только необходимые права доступа для выполнения своих рабочих обязанностей. Управление доступом может осуществляться с помощью ролевой модели или других методов для определения прав доступа.

**Вывод:**

Политика безопасности является основой мер административного уровня, направленных на защиту информации и связанных с ней ресурсов в организации. Для эффективного построения системы защиты информации необходимо определить границы системы, ресурсы, подлежащие защите, и технологию обработки информации и решаемые задачи. Оценка рисков включает идентификацию угроз и уязвимостей, а также оценку существующих и предполагаемых средств обеспечения информационной безопасности. На основе оценки рисков могут быть предприняты соответствующие меры для обеспечения информационной безопасности, такие как разработка политики информационной безопасности, установка антивирусного программного обеспечения, регулярное резервное копирование данных, обучение персонала и мониторинг сетевой активности. Оценка рисков и принятие соответствующих мер по обеспечению информационной безопасности являются важными шагами для защиты конфиденциальной информации и предотвращения возможных инцидентов.