Учреждение образования

«Белорусский государственный технологический университет»

**Практическое занятие №2**

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

Выполнил:

Студент 2 курса 2 группы ФИТ

Авдей Алексей

Цель: разработать проект политики информационной безопасности бизнес-компании.

**Введение**

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 безопасности** организации образует совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области **безопасности**, которые регулируют управление, защиту и распределение ценной информации. Кроме этого в политику безопасности входят требования в адрес субъектов информационных отношений и излагается политика ролей субъектов информационных отношений

Из-за возможности утечки информации или неосторожного поведения сотрудников компания теряет свою конкурентоспособность на рынке. Благодаря разработке различных систем защиты это можно минимизировать или вовсе избежать. При разработке системы защиты необходимо опираться на различные стандарты, которые позволят взаимодействовать с разными государственными органами в соответствующем правовом поле, а также успешно сотрудничать с зарубежными партнёрами.

Основная задача политики безопасности — это задокументировать правила работы на предприятии в области информационной безопасности. Без нее взаимодействие работников с различными ресурсами будет регулироваться лишь неформально и поэтому возрастет риск нарушений и утечек данных. Поэтому минимизация рисков компании приведёт к повышению её прибыльности.

**Описание структуры Компании**

**1.1. Организационная структура.**

Университет представляет собой слаженную структуру, включающую ректорат, факультеты, библиотеки, научно-исследовательские лаборатории и административные службы. Вся организация функционирует как единое целое, и безопасность данных и информационных ресурсов становится крайне важной.

* Организационная структура дает четкое понимание того, в каком направлении движется компания. Ясная структура — это инструмент, с помощью которого можно придерживаться порядка в принятии решений и преодолевать различные разногласия.
* Организационная структура связывает участников. Благодаря ей люди, присоединяющиеся к группе, имеют отличительные черты. В то же время и сама группа обладает определенными особенностями.
* Организационная структура формируется неизбежно. Любая организация по определению подразумевает какую-то структуру.

Организационная структура Университета.

1. Ректорат: В состав ректората входят ректор университета и его заместители. Ректорат управляет всей деятельностью университета, разрабатывает стратегические планы и принимает стратегические решения.

2. Факультеты: Университет имеет несколько факультетов, каждый из которых специализируется в определенной области знаний. Каждый факультет включает в себя деканат, который руководит образовательными программами и активно взаимодействует с преподавателями и студентами.

3. Научно-исследовательские лаборатории: Университет поддерживает научно-исследовательскую деятельность и включает в себя несколько лабораторий, где проводятся исследования в различных областях.

4. Библиотеки: Университет обеспечивает доступ к библиотечным ресурсам и информационным системам, которые поддерживают учебный процесс и научные исследования.

5. Административные службы: Университет также включает в себя административные службы, которые занимаются финансами, кадрами, информационными технологиями, организацией мероприятий и другими аспектами управления университетом.

Таким образом, организационная структура вашего университета включает в себя ректорат, факультеты, научно-исследовательские лаборатории, библиотеки и административные службы, и она ориентирована на поддержание академической и научной деятельности, а также обеспечение безопасности данных и информационных ресурсов.

**1.2. Информационные системы и данные.**

Все структурные подразделения университета взаимодействуют с помощью информационных систем, которые обеспечивают хранение, передачу и анализ данных. Это включает в себя системы управления обучением, хранение личных данных студентов, финансовые системы и системы управления исследованиями.

**1.3. Организационная культура.**

Университет считает информационную безопасность приоритетом и строит организационную культуру, основанную на осознании важности безопасности данных. Эта культура вдохновляет сотрудников и студентов на соблюдение политики информационной безопасности.

**Оценка рисков**

Способы нанесения вреда информационным системам модифицируются и усложняются с каждым годом. Всё чаще используются специально написанные программы, эксплуатируются скрытые угрозы, а традиционные методы атак всё чаще исправляются при разработке программ и в итоге не используются для эксплуатации. Все этим угрозы проникают внутрь сети — на уровень ядра, уровень доступа пользователей, где защита от угроз может находиться на минимальном уровне. С этой позиции угрозы без проблем могут перейти на новый уровень и в итоге добираются до своей цели — конкретные ресурсы в сети или информация. Цель современных кибер-угроз чаще всего заключается в захвате ценной информации и дальнейшей её эксплуатации или продаже, также целью может быть шантаж или вымогательство.

Второй этап разработки проекта политики информационной безопасности Университета включает в себя оценку рисков. Оценка рисков необходима для выявления потенциальных угроз, оценки уязвимостей и анализа возможных последствий нарушения информационной безопасности.

2.1. Идентификация угроз

Идентификация угроз - первый шаг в оценке рисков. На данном этапе проводится анализ различных угроз, которые могут повлиять на информационную безопасность Университета. Это могут быть как внутренние, так и внешние угрозы. Примеры угроз включают в себя:

- Несанкционированный доступ к конфиденциальным данным.

- Атаки на информационные системы и сети.

- Утеря или кража устройств, содержащих конфиденциальную информацию.

- Вредоносные программы (вирусы, трояны и др.).

- Социальная инженерия (фишинг и атаки с использованием манипуляции сотрудников).

2.2. Оценка уязвимостей

После идентификации угроз проводится оценка уязвимостей, которые могут быть использованы злоумышленниками для реализации угроз. Уязвимости могут относиться как к техническим аспектам (например, уязвимости программного обеспечения), так и к человеческому фактору (например, несоблюдение политики паролей сотрудниками).

2.3. Анализ последствий

Анализ последствий позволяет оценить потенциальные последствия нарушения информационной безопасности. Это включает в себя следующие аспекты:

- Потеря конфиденциальных данных.

- Повреждение информационных систем и инфраструктуры.

- Репутационные и финансовые потери для Университета.

- Юридические последствия и возможные штрафы.

Анализ последствий помогает определить, насколько критичными являются угрозы и уязвимости и какие меры защиты необходимо принимать для их минимизации.

На основе результатов идентификации угроз, оценки уязвимостей и анализа последствий разрабатываются меры защиты, которые включаются в проект политики информационной безопасности. Эти меры направлены на предотвращение и снижение рисков информационной безопасности и обеспечение надежной защиты данных и информационных ресурсов Университета.

**Разработка мер защиты**

3.1. Политика доступа

Разработана политика управления доступом, которая определяет права доступа для сотрудников и студентов в соответствии с их ролями и обязанностями.

3.2. Обучение и осведомленность

Внедрена обучающая программа по информационной безопасности для всех сотрудников и студентов. Обучение проводится регулярно для повышения уровня осведомленности.

3.3. Мониторинг и аудит

Установлены системы мониторинга и аудита, которые помогают выявлять аномалии и реагировать на них.

3.4. Защита данных

Приняты меры по защите данных, включая шифрование, регулярное резервное копирование и физическую защиту серверных помещений.

**Выводы**

Разработка проекта политики информационной безопасности Университета представляет собой важный шаг в обеспечении защиты конфиденциальных данных, обеспечении надежности информационных ресурсов и создании безопасной среды для всех членов университетского сообщества. Проект политики информационной безопасности составлен с учетом современных стандартов и лучших практик в области информационной безопасности.

Оценка рисков позволила выявить потенциальные угрозы и уязвимости, которые могут повлиять на безопасность данных и работоспособность информационных систем. Разработка мер защиты включает в себя установление строгих правил управления доступом, обеспечение обучения сотрудников и студентов, а также создание процедур реагирования на инциденты информационной безопасности.

Организационная культура Университета, основанная на ценностях открытости, интеллектуального развития, сотрудничества и ответственности, служит основой для успешной реализации политики информационной безопасности. Она поддерживает осознание рисков и активное участие всех членов университетского сообщества в обеспечении безопасности данных.

Соблюдение политики информационной безопасности является обязательным для всех сотрудников и студентов Университета, и это требует сознательности и ответственности каждого. Обучение и осведомленность считаются ключевыми факторами в обеспечении безопасности данных и информационных ресурсов.

В целом, проект политики информационной безопасности Университета создает основу для обеспечения надежной защиты данных и информационных ресурсов, способствует развитию безопасной и образовательной среды и поддерживает цели и ценности Университета.

**Приложение A: Политика управления доступом**

**Политика управления доступом**

Цель:

Целью данной политики является обеспечение безопасного и контролируемого доступа к информационным ресурсам Университета, минимизация угроз и рисков информационной безопасности.

**Область действия:**

Данная политика применяется ко всем сотрудникам, студентам и сторонним лицам, имеющим доступ к информационным ресурсам Университета.

**Права доступа:**

1. Права доступа к информационным ресурсам определяются на основе ролей и обязанностей сотрудников и студентов.

2. Права доступа могут быть предоставлены, изменены или отозваны только после получения официального разрешения от ответственных лиц.

3. Все пользователи обязаны соблюдать принципы минимального доступа и использовать предоставленные им права только для целей, предусмотренных их обязанностями.

**Аутентификация и авторизация:**

1. Все пользователи обязаны использовать надежные методы аутентификации, такие как пароли, биометрические данные и двухфакторную аутентификацию.

2. Пользователи не имеют права передавать свои учетные данные третьим лицам.

3. Учетные записи пользователей могут быть заблокированы или приостановлены в случае нарушения политики информационной безопасности.

**Мониторинг и аудит:**

1. Ведется мониторинг действий пользователей в информационных системах с целью выявления аномалий и несанкционированных действий.

2. Проводятся регулярные аудиты прав доступа для подтверждения их актуальности и соответствия политике.

Санкции:

1. Нарушения политики управления доступом могут привести к дисциплинарным мерам вплоть до увольнения сотрудников или исключения студентов.

2. Сотрудники и студенты могут быть подвергнуты юридической ответственности в случае совершения действий, противоречащих данной политике.

Действие:

Данная политика вступает в силу с момента утверждения и подлежит регулярной пересмотру и обновлению для обеспечения актуальности и эффективности.

**Приложение B: Программа обучения по информационной безопасности**

Программа обучения по информационной безопасности

Цель:

Целью программы обучения по информационной безопасности является повышение уровня осведомленности и знаний всех сотрудников и студентов Университета в области информационной безопасности.

**Содержание:**

1. Введение в информационную безопасность.

2. Аутентификация и авторизация.

3. Защита данных и шифрование.

4. Сетевая безопасность и защита от вредоносных программ.

5. Социальная инженерия и защита от фишинга.

6. Управление рисками и обеспечение бизнес-континуитета.

7. Правила использования информационных ресурсов Университета.

8. Процедуры реагирования на инциденты информационной безопасности.

**Методы обучения:**

1. Лекции и семинары.

2. Онлайн-курсы и видеоматериалы.

3. Практические занятия и тренировки.

**Обязанности участников:**

1. Все сотрудники и студенты обязаны пройти обучение по информационной безопасности в течение первых 30 дней после приема на работу или зачисления в университет.

2. Обучение по информационной безопасности должно проводиться ежегодно для всех пользователей.

3. Пользователи обязаны соблюдать правила и рекомендации, изложенные в программе обучения.

**Приложение C: Соглашение о конфиденциальности данных**

Соглашение о конфиденциальности данных

Цель:

Целью данного соглашения является установление правил и обязательств по обработке и защите конфиденциальных данных в Университете.

Действие:

1. Конфиденциальные данные могут быть собраны только с согласия субъектов данных и использованы только в целях, указанных в согласии.

2. Конфиденциальные данные должны храниться и передаваться с использованием надежных методов защиты, включая шифрование и физическую защиту.

3. Доступ к конфиденциальным данным предоставляется только сотрудникам и студентам, уполномоченным на основании политики управления доступом.

**Сохранение данных:**

1. Конфиденциальные данные должны храниться в течение определенного срока, после чего они должны быть уничтожены или анонимизированы.

2. Субъекты данных имеют право запросить доступ к своим конфиденциальным данным и внести корректировки в них.

**Санкции**:

1. Нарушения соглашения о конфиденциальности данных могут привести к дисциплинарным мерам и юридической ответственности в соответствии с действующим законодательством.

Действие:

Данное соглашение вступает в силу с момента подписания и остается в силе до момента его отмены.