УО «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра «Информационных систем и технологий»

Специальность 1-40 05 01 «Информационные Системы и Технологии»

**Основы информационной безопасности**

**Практическое задание № 2**

**Вариант 17**

|  |  |  |  |
| --- | --- | --- | --- |
| **Выполнил** |  |  |  |
| Студент 2 курса группы 1 |  |  | Д.И. Велютич |
|  | подпись, дата |  | инициалы и фамилия |
| **Проверил(а)** |  |  | Н.В. Ржеутская |
|  | подпись, дата |  | инициалы и фамилия |

Минск 2023

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

Цель: Разработать проект политики информационной безопасности бизнес-компании.

**Теория**

Меры административного уровня, которые принимает руководство организации, основаны на их политике безопасности. Эта политика - это совокупность управленческих решений, направленных на защиту информации и связанных с ней ресурсов. Она определяет стратегию организации в области информационной безопасности и решает, сколько ресурсов следует выделить на эту цель.

Чтобы определить политику информационной безопасности, нужно выполнить следующие шаги:

1. Определить документы и стандарты в области информационной безопасности, а также основные аспекты политики, такие как управление доступом, антивирусная защита, резервное копирование, восстановительные работы и информирование о инцидентах.

2. Решить, как управлять рисками: проводить ли полный анализ рисков или ограничиться базовыми мерами безопасности.

3. Структурировать меры безопасности по уровням.

4. Установить процедуру сертификации согласно стандартам в области информационной безопасности. Также нужно определить, как часто проводить совещания руководства по вопросам информационной безопасности и как обучать пользователей системы в этой области.

Для создания системы защиты информации необходимо определить границы системы, для которой требуется обеспечить информационную безопасность. Система управления информационной безопасностью должна строиться в пределах этих границ.

Описание границ системы может включать следующие пункты:

1. Структура организации и планируемые изменения в связи с разработкой или модернизацией системы обработки информации.

2. Размещение компьютерной техники и связанной инфраструктуры, включая иерархию оборудования.

3. Ресурсы информационной системы, которые нуждаются в защите, такие как компьютерное оборудование, данные и программное обеспечение. Все эти ресурсы имеют ценность для организации и должны быть оценены с помощью системы критериев.

4. Технология обработки информации и задачи, которые выполняются в системе. Должны быть созданы модели обработки информации с учетом ресурсов.

В результате этого анализа будет создан документ, который содержит информацию о границах системы, защищаемых ресурсах и системе критериев для оценки их ценности.

Базовый уровень информационной безопасности соответствует минимальным требованиям. Обычно он используется в типовых проектах. На этом уровне рассматриваются типичные угрозы, такие как вирусы, сбои оборудования и несанкционированный доступ. Для их предотвращения необходимы стандартные меры безопасности, независимо от вероятности их возникновения и уязвимостей ресурсов. Поэтому на базовом уровне не требуется детального анализа угроз.

Когда нарушения информационной безопасности могут иметь серьезные последствия, базовый уровень требований к режиму информационной безопасности становится недостаточным. Для установления дополнительных требований нужно:

1. Определить ценность ресурсов.

2. Расширить стандартный набор угроз, учитывая специфику информационной системы.

3. Оценить вероятность возникновения угроз.

4. Определить уровень уязвимости ресурсов.

Политика безопасности строится на основе анализа рисков, считаемых реальными для информационной системы организации. После анализа рисков и разработки стратегии защиты, создается программа безопасности. Эта программа выделяет ресурсы, назначает ответственных и устанавливает процедуры контроля ее выполнения.

Существуют разные методы оценки рисков, выбор которых зависит от уровня требований организации, характера угроз и эффективности возможных мер безопасности.

Процесс оценки рисков включает следующие этапы:

1. Идентификация и оценка ресурсов.

2. Оценка угроз.

3. Оценка уязвимостей.

4. Оценка средств обеспечения безопасности.

5. Оценка рисков.

Ресурсы, которые имеют ценность для организации и уязвимы, рассматриваются как подверженные риску при наличии угрозы. При оценке рисков учитываются потенциальные негативные последствия от нежелательных событий и степень уязвимости ресурсов к этим угрозам.

Риск отражает опасность для системы и организации, зависящую от ценности ресурсов, вероятности угроз и уровня уязвимости.

Цель оценки рисков - определение характеристик рисков для информационной системы и ее ресурсов, чтобы выбрать необходимые меры управления информационной безопасностью.

Оценка рисков учитывает:

- Ценность ресурсов.

- Оценку значимости угроз.

- Эффективность средств защиты.

Ценность ресурсов и потенциальное негативное воздействие на организацию можно определять качественно (например, как опасно или безопасно) или количественно (например, в денежных единицах).

Вероятность угрозы зависит от факторов, таких как привлекательность ресурсов, возможность получения выгоды, технические возможности угрозы, вероятность ее реализации и степень уязвимости ресурсов.

Граница между приемлемыми и неприемлемыми рисками определяется пользователями и зависит от конкретной организации.

На основе политики безопасности разрабатывается программа безопасности, которая реализуется на процедурном и программно-техническом уровнях.

Процедурные меры безопасности включают:

- Управление персоналом.

- Физическую защиту.

- Обеспечение работоспособности.

- Реагирование на нарушения безопасности.

- Планирование восстановительных работ.

На программно-техническом уровне используются механизмы безопасности, такие как идентификация пользователей, управление доступом, аудит, криптография и др.

Управление информационной системой и мерами безопасности должно быть в соответствии с общепринятыми стандартами и учитывать сетевые угрозы, а также специфику услуг и сервисов.

**Условия задачи**

Разработать проект политики информационной безопасности бизнес-компании, оформив результаты в виде пояснительной записки. Пояснительная записка может, например, содержать следующие разделы:

1. Титульный лист;
2. Введение (обосновывается важность разработки политики информационной безопасности);
3. Описание структуры бизнес-компании (выбор компании предварительно согласовывается с преподавателем);
4. Оценка рисков;
5. Разработка мер защиты;
6. Выводы.

Электронный вариант вносится в электронную тетрадь и показывается преподавателю для предварительной проверки (объем – 10-20 страниц).

После предварительной проверки пояснительная записка распечатывается и проект политики информационной безопасности бизнес-компании защищается в указанные преподавателем сроки.

Варианты индивидуальных заданий:

**Вариант 17: Военкомат**

**Исполнительная часть**

**Разработка политики информационной безопасности для Военкомата**

**1. Введение**

В современном мире, где информационные технологии проникают во все сферы деятельности, вопросы информационной безопасности становятся более актуальными и важными, чем когда-либо. Рост зависимости от цифровых технологий сопровождается увеличением потенциальных угроз, связанных с ними. Для организаций, особенно органов государственной власти, таких как Военкомат, обеспечение конфиденциальности, целостности и доступности данных становится первостепенной задачей.

Осознание того, что даже кратковременная утечка информации или недоступность важных данных может серьезно повлиять на выполнение своих обязанностей, делает вопрос информационной безопасности в Военкомате более чем актуальным. Нарушение безопасности данных может не только ущемить интересы организации, но и иметь долгосрочные последствия для граждан, подлежащих призыву на военную службу.

Разработка и внедрение политики информационной безопасности становятся неотъемлемой частью его деятельности, направленной на защиту интересов государства и обеспечение безопасности граждан.

**2. Описание структуры Военкомата**

Прежде чем перейти к разработке политики информационной безопасности, давайте более подробно рассмотрим структуру Военкомата. Военкомат - это государственная организация, ответственная за мобилизационную подготовку и учет граждан, подлежащих призыву на военную службу.

Организация функционирует в соответствии с законодательством и нормативными актами, регулирующими вопросы призыва и воинской службы граждан. Военкомат выполняет следующие ключевые функции:

* **Штаб Военкомата:** Ключевой орган управления, отвечающий за разработку стратегии и координацию деятельности остальных подразделений. Штаб взаимодействует с органами государственной власти и регулирующими организациями.
* **Отдел регистрации и учета граждан:** Занимается регистрацией и ведением учета граждан в возрасте призыва. Основной задачей отдела является подготовка реестров и баз данных граждан, подлежащих призыву, а также выдача воинских билетов и повесток.
* **Отдел по военной службе:** Отвечает за организацию призыва граждан на военную службу, их медицинское освидетельствование и отправку в воинские части. Отдел ведет учет местонахождения призывников и контролирует исполнение ими воинских обязанностей.
* **Отдел информационных технологий и связи:** Осуществляет управление информационными системами и обеспечивает связь внутри Военкомата и с другими органами государственной власти. Отдел ответственен за хранение, обработку и передачу важных данных, связанных с призывом и военной службой граждан.

Структура Военкомата обеспечивает эффективное выполнение его задач и функций, но при этом также создает необходимость в разработке и внедрении эффективных мер информационной безопасности, чтобы гарантировать защиту конфиденциальных данных и бесперебойное функционирование информационных систем.

**3. Оценка рисков**

Перейдем к важному этапу разработки политики информационной безопасности - оценке рисков. Важно понимать, какие угрозы могут возникнуть и какие данные подвергаются наибольшему риску. В случае Военкомата, основными аспектами оценки рисков являются:

* **Ценность данных:** Главной ценностью являются данные о гражданах, включая их личные сведения и воинские категории. Утрата или утечка таких данных может иметь серьезные последствия, включая ущемление прав и интересов граждан, а также нарушение законодательства о защите персональных данных.
* **Угрозы:** Потенциальные угрозы могут включать несанкционированный доступ к данным, вирусные атаки, утечки информации и физические угрозы для серверов и оборудования. Угрозы могут происходить как изнутри (например, неаккуратное обращение с данными со стороны сотрудников), так и извне (например, хакерские атаки).
* **Вероятность и последствия угроз:** Необходимо оценить вероятность возникновения угроз и потенциальные последствия для безопасности данных. Например, какова вероятность утечки личных данных граждан, и какие могут быть последствия этой утечки? Важно учитывать не только технические аспекты, но и человеческий фактор, так как многие инциденты информационной безопасности могут быть вызваны небрежностью или недобросовестными действиями сотрудников.
* **Уязвимости:** Важно определить уязвимости в существующей информационной инфраструктуре и процессах. Устаревшее программное обеспечение, недостаточные меры защиты, неправильно настроенные права доступа и недостаточная обученность персонала могут быть уязвимыми местами. Идентификация уязвимостей позволяет разработать соответствующие меры защиты.

Оценка рисков позволит выявить приоритетные направления для разработки политики информационной безопасности и определить, какие меры защиты следует предпринять для минимизации рисков. Результаты оценки рисков будут использоваться для формулировки конкретных положений политики информационной безопасности и разработки мероприятий по ее внедрению.

**4. Разработка мер защиты**

На основе оценки рисков разрабатываются конкретные меры защиты для Военкомата. Важно подчеркнуть, что политика информационной безопасности не ограничивается только техническими мерами, она также включает в себя процедурные и организационные аспекты. Некоторые из важных мер могут включать:

* **Установка средств защиты:** Это включает в себя использование современных антивирусных программ, брандмауэров, а также средств шифрования данных для защиты конфиденциальной информации. Регулярное обновление и мониторинг этих средств также является важной составляющей.
* **Авторизация и аутентификация:** Внедрение систем авторизации и аутентификации для контроля доступа к данным. Каждый сотрудник Военкомата должен иметь уникальный идентификационный код и пароль для доступа к системам. Дополнительные механизмы множественной аутентификации могут быть введены для повышения безопасности доступа.
* **Обучение сотрудников:** Регулярное обучение сотрудников организации в вопросах информационной безопасности. Сотрудники должны быть в курсе правил и процедур безопасности, а также знать, как распознавать потенциальные угрозы и действовать в случае инцидентов.
* **Физическая безопасность:** Обеспечение безопасности серверных помещений и оборудования. Доступ к серверам должен быть строго ограничен и контролируем. Применение систем видеонаблюдения и системы контроля доступа может усилить физическую безопасность.
* **Регулярное аудирование и мониторинг:** Проведение аудита систем безопасности и мониторинга активности с целью выявления несанкционированных действий. Это позволяет реагировать на потенциальные угрозы в реальном времени и предпринимать необходимые меры.
* **Разработка инцидентных планов:** Создание планов действий в случае возникновения инцидентов информационной безопасности. Определение цепочки командования, процедур уведомления и восстановления после инцидента.
* **Регулярное обновление политики:** Политика информационной безопасности должна регулярно обновляться и адаптироваться к изменяющимся угрозам и технологическим изменениям. Это позволяет оставаться на шаг впереди потенциальных атакующих.
* **Сотрудничество с внешними экспертами:** Важно также устанавливать сотрудничество с внешними экспертами и организациями по вопросам информационной безопасности для получения актуальных рекомендаций и поддержки.

Реализация этих мер позволит Военкомату обеспечить надежную защиту информации, сохранить конфиденциальность и целостность данных, а также обеспечить доступность информационных ресурсов в рамках законодательных и организационных требований.

**5. Выводы**

Разработка и внедрение политики информационной безопасности в Военкомате имеют высшую стратегическую значимость для обеспечения национальной безопасности и надежной работы данной организации. В ходе разработки данной политики были рассмотрены важные аспекты, которые позволяют обеспечить конфиденциальность, целостность и доступность данных, а также предотвратить потенциальные угрозы.

Важно подчеркнуть, что информационная безопасность не ограничивается только техническими мерами защиты, но также включает в себя обучение сотрудников, процедурные аспекты и организационные изменения. Все эти компоненты взаимосвязаны и взаимодействуют для создания надежной системы защиты информации.

Регулярное обновление и адаптация политики информационной безопасности к изменяющимся условиям и угрозам являются ключевыми моментами в обеспечении её эффективности. Также важным аспектом является сотрудничество с внешними экспертами и организациями по вопросам информационной безопасности, что позволяет получать актуальные рекомендации и поддержку.

Внедрение и строгое соблюдение политики информационной безопасности Военкомата являются не только обязательством перед государством, но и залогом сохранности важных данных и обеспечения национальной безопасности. Эти меры способствуют сохранению доверия граждан к организации и обеспечению её бесперебойной деятельности в условиях современных информационных вызовов и угроз.