Сделал:
Тарасов Константин

Политика информационной безопасности

Безопасности в классе

2024 г.

Политика информационной безопасности

1. Оглавление

2. Введение

Политика информационной безопасности - это стратегия и набор правил, направленных на защиту конфиденциальности, целостности и доступности информации в организации.

3. Обозначения и сокращения

Вот некоторые обозначения и сокращения, которые используются в политике информационной безопасности:

- АИБ — администратор информационной безопасности;
- ИБ — информационная безопасность;
- ИР — информационные ресурсы;
- ИС — информационная система;
- НСД — несанкционированный доступ;
- СЗИ — средство защиты информации;
- СУИБ — система управления информационной безопасностью;
- ЭВМ — электронная вычислительная машина.

4. Термины и определения

Информационная политика — универсальный социальный ме-ханизм определения целей, задач, принципов и условий реализации приоритетов общественного развития в информационной сфере, основанный на конкурентной публичной борьбе субъектов поли-тики и связанный с реализацией общественной поддержки субъ-ектов политики и их представлений о содержании общественно-го блага и путях его достижения.

Информационная безопасность — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая).

5. Цели и задачи

- Освоение темы и свод правил за ПК используемые в колледже ЧПУО. КГК;
- Понятие правил;
- Своевременное выявление, оценка и прогнозирование источников угроз ИБ
- Создание механизма оперативного реагирования на угрозы ИБ;
- Предотвращение и/или снижение ущерба от реализации угроз ИБ;
- Защита от вмешательства в процесс функционирования ИС посторонних лиц;
- Выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников.

6. Область применения

1. АИБ — администратор информационной безопасности: Область применения в управлении информационной безопасностью, наблюдение за безопасностью информационных систем.

2. ИБ — информационная безопасность: Область применения в защите информации от несанкционированного доступа, обеспечении конфиденциальности, целостности и доступности данных.

3. ИР — информационные ресурсы: Область применения в управлении и использовании информационных ресурсов организации.

4. ИС — информационная система: Область применения в разработке, эксплуатации и поддержке информационных систем.

5. НСД — несанкционированный доступ: Область применения в предотвращении и выявлении несанкционированного доступа к информации.

6. СЗИ — средство защиты информации: Область применения в обеспечении защиты информации при ее хранении, передаче и обработке.

7. СУИБ — система управления информационной безопасностью: Область применения в планировании, внедрении и контроле мер по обеспечению информационной безопасности.

8. ЭВМ — электронная вычислительная машина: Область применения в обработке информации с использованием компьютерной техники.

6.1 Защита конфиденциальности данных

1. Шифрование данных
2. Управление доступом
3. Анонимизация персональных данных
4. Защита от несанкционированного доступа
5. Политика конфиденциальности

6.2 Предотвращение несанкционированного доступа к информации

1. Использование сильных паролей и их регулярное обновление.
2. Установка многофакторной аутентификации.
3. Шифрование конфиденциальных данных.
4. Регулярные аудиты безопасности и мониторинг доступа к информации.
5. Обучение сотрудников правилам безопасности информации.

6.3 Обеспечение целостности данных и систем

Обеспечение целостности данных и систем включает в себя использование методов шифрования, контрольных сумм, а также управление доступом и аутентификацию.

6.4 Защита от вредоносных программ и кибератак

1. Установите антивирусное программное обеспечение и регулярно обновляйте его.
2. Используйте сильные пароли и двухфакторную аутентификацию.
3. Обновляйте операционную систему и программное обеспечение.
4. Будьте осторожны при открытии вложений в электронной почте или переходе по подозрительным ссылкам.
5. Регулярно делайте резервные копии важных данных.

6.5 Обеспечение безопасности сетей и коммуникаций

1. Использование сильных паролей и многофакторной аутентификации.
2. Шифрование данных в публичных сетях.
3. Регулярное обновление программного обеспечения для закрытия уязвимостей.
4. Мониторинг сетевого трафика для выявления подозрительной активности.
5. Обучение сотрудников основам кибербезопасности.

7. Физические нарушения, способы избежания

- Политика информационной безопасности фокусируется на защите информации от несанкционированного доступа, использования, раскрытия, изменения или уничтожения. Физические нарушения включают несанкционированный доступ к оборудованию или помещениям, кражу

информационных носителей и другие физические угрозы. Способы избежания включают контроль доступа, видеонаблюдение, использование замков и прочих средств защиты.

7.1 Физическая защита информационных ресурсов

Физическая безопасность информационных ресурсов — это комплекс информационно-технических мероприятий, направленных на защиту от неавторизованного доступа, повреждения и воздействия в отношении помещений и информации организации.

Основные средства обеспечения физической безопасности информационных ресурсов включают:

Нормативное обеспечение: разработку, документирование и периодическое обновление политики физической защиты и защиты среды информационной системы.

Управление физическим доступом: использование системы управления доступом во всех точках доступа к информационным ресурсам и активам, определение периметров безопасности для защиты помещений и зон расположения средств обработки информации.

Мониторинг физического доступа: использование устройств наблюдения и сигнализации реального времени, автоматизированных средств для распознания нарушений и инициирования ответных действий.

Защита оборудования: обеспечение противопожарной защиты, защиты от других экологических и техногенных катастроф, обеспечение защиты телекоммуникационных кабельных сетей от перехвата информации или повреждения.

Контроль посетителей: выделение зоны регистрации, сопровождение всех посетителей на объектах, ведение журналов учета доступа.

7.2 Контроль доступа к помещениям и оборудованию

Политика информационной безопасности обычно включает в себя контроль доступа к помещениям и оборудованию через использование различных методов, таких как ключевые карты, биометрическая идентификация, пароли и т. д.

7.3 Методы предотвращения кражи информационных носителей

1. Шифрование данных на информационных носителях.
2. Установка систем контроля доступа и мониторинга.
3. Физическая защита помещений, где хранятся информационные носители.
4. Обучение сотрудников правилам безопасности и контроля за информацией.
5. Использование меток и инвентаризации для отслеживания информационных носителей.

8. Уязвимость в сети

Политика информационной безопасности - это набор мер и правил, направленных на защиту информации от угроз и обеспечение конфиденциальности, целостности и доступности данных.
Уязвимость в сети - это слабое место или недостаток в системе, который может быть использован злоумышленником для нарушения безопасности.

8.1 Проактивное управление уязвимостями в информационных системах

Политика информационной безопасности включает проактивное управление уязвимостями в информационных системах.

8.2 Влияние регулирования на политику информационной безопасности

Регулирование может определять требования к защите информации и влиять на разработку политики информационной безопасности.

8.3 Комплексный подход к защите от угроз в сети

Политика информационной безопасности - это комплексный подход к защите от угроз в сети.

8.4 Роль обучения и осведомленности сотрудников в предотвращении уязвимостей

Политика информационной безопасности определяет правила и процедуры для защиты информации. Обучение сотрудников играет ключевую роль в предотвращении уязвимостей, так как осведомленные сотрудники могут помочь выявить и предотвратить потенциальные угрозы информационной безопасности.

8.5 Технологические инновации в области обнаружения и устранения уязвимостей

1. Развитие технологий обнаружения уязвимостей.
2. Применение машинного обучения для выявления потенциальных угроз.
3. Усовершенствование методов криптографии и защиты данных.

4. Обеспечение безопасности Интернета вещей (IoT).
5. Развитие систем мониторинга и реагирования на инциденты информационной безопасности.

9. Правила в компьютерном классе

1. Следуйте инструкциям учителя.
2. Не устанавливайте программное обеспечение без разрешения.
3. Берегите компьютерное оборудование.
4. Соблюдайте правила использования интернета и социальных сетей.
5. Не копируйте или распространяйте чужие работы без разрешения.

10. Правила работы за компьютером

1. Соблюдайте правила информационной безопасности.
2. Используйте лицензионное программное обеспечение.
3. Соблюдайте политику конфиденциальности и защиты данных.
4. Следите за эргономикой рабочего места.
5. Выполняйте бэкапы важных данных.
6. Соблюдайте правила использования сети и интернета.