



ОЦЕНКА ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УЧРЕЖДЕНИИ ФЕДЕРАЛЬНОГО ОРГАНА ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ В УСЛОВИЯХ ПЕРЕХОДА НА ОТЕЧЕСТВЕННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Орлова Елена Валерьевна

студент, Российский экономический университет им. Г.В. Плеханова
РФ, г. Москва

Сизов Валерий Александрович

научный руководитель, Российский экономический университет
им. Г.В. Плеханова
РФ, г. Москва

Аннотация

В статье рассматриваются проблемы обеспечения информационной безопасности в учреждениях федеральных органов исполнительной власти при переходе на отечественное программное обеспечение (ПО). Особое внимание уделено анализу эффективности мер безопасности в условиях использования национальных решений, а также сопоставлению их с зарубежными аналогами. Проводится оценка уровня угроз, связанных с переходом на отечественное ПО, и вырабатываются рекомендации по повышению защиты информационных систем и данных, хранимых в таких учреждениях.

Ключевые слова: информационная безопасность, отечественное программное обеспечение, федеральные органы исполнительной власти, защита данных, киберугрозы, безопасность ПО, национальная безопасность.

1. Введение

С переходом на отечественное программное обеспечение (ПО) в государственных и муниципальных учреждениях возникает ряд вызовов, связанных с обеспечением информационной безопасности. В условиях цифровизации государственных процессов и растущих угроз в сфере кибербезопасности, важно не только обеспечить защиту данных, но и гарантировать работоспособность и совместимость ПО с различными системами. Этот переход становится особенно актуальным для федеральных органов исполнительной власти, где безопасность данных и устойчивость работы системы имеют критическое значение.

2. Проблемы и задачи обеспечения информационной безопасности

Переход на отечественное ПО представляет собой не только технологический, но и организационный вызов. Во-первых, важно отметить потенциальные уязвимости, которые могут возникать при замене зарубежных решений на отечественные, включая риски недостаточной зрелости национальных технологий и проблемы совместимости с существующими системами. Во-вторых, необходимо обеспечить высокий уровень защиты данных, поскольку деятельность органов исполнительной власти связана с обработкой конфиденциальной информации, которая требует дополнительных мер по защите от внешних и внутренних угроз.

Задачами оценки эффективности обеспечения информационной безопасности в данном контексте являются:

- Анализ текущих угроз информационной безопасности в учреждениях, использующих отечественное ПО.
- Оценка уровня защищенности данных в условиях перехода на отечественные решения.
- Сравнение отечественного ПО с зарубежными аналогами по уровням безопасности и функциональности.
- Разработка рекомендаций по повышению безопасности при внедрении отечественного ПО.

3. Меры обеспечения информационной безопасности при переходе на отечественное ПО

Для обеспечения информационной безопасности в условиях перехода на отечественное ПО необходимо учитывать следующие ключевые аспекты:

3.1. Оценка уровня угроз и рисков

Переход на отечественное ПО может сопряжен с рядом рисков, включая несовершенство систем защиты, отсутствие интеграции с международными стандартами безопасности и недостаточное тестирование отечественных продуктов на уязвимости. Для минимизации этих рисков необходимо провести комплексную оценку угроз, в том числе:

- Возможные кибератаки на системы и данные.
- Утечка конфиденциальной информации через уязвимости ПО.
- Проблемы с совместимостью отечественного ПО с имеющимися решениями.

3.2. Разработка и внедрение политик безопасности

Важной мерой является создание и внедрение четких политик информационной безопасности, включающих требования к защите данных, контроль за доступом и регулярную проверку уязвимостей. Это включает в себя:

- Установление стандартов по защите конфиденциальности и целостности данных.
- Создание централизованных систем мониторинга и контроля.
- Проведение регулярных аудитов безопасности и тестирования ПО на наличие уязвимостей.

3.3. Использование криптографических методов защиты

Криптографические методы являются неотъемлемой частью обеспечения безопасности информации. Для защиты данных, особенно в контексте перехода на отечественное ПО, важно использовать отечественные решения для шифрования и аутентификации, которые обеспечат высокий уровень защиты. Это включает:

- Применение отечественных сертифицированных криптографических алгоритмов.
- Реализация многофакторной аутентификации пользователей.
- Обеспечение безопасности канала передачи данных.

3.4. Обучение и повышение осведомленности сотрудников

Одной из важнейших составляющих информационной безопасности является обучение сотрудников. Это включает:

- Проводить регулярные тренинги по безопасности.
- Разрабатывать и внедрять систему предотвращения человеческих ошибок.
- Обучать сотрудников правильным методам работы с конфиденциальной информацией.

4. Сравнение отечественного ПО с зарубежными аналогами

Анализ эффективности отечественного ПО по сравнению с зарубежными решениями позволяет выявить следующие ключевые различия:

4.1. Безопасность

Отечественное ПО, как правило, менее подвержено влиянию внешних угроз, связанных с установкой зарубежных программных продуктов, однако оно может иметь менее развитую систему защиты от специфических угроз, таких как zero-day уязвимости. Важно, чтобы отечественное ПО проходило регулярные тесты на уязвимости и сертификацию в области кибербезопасности.

4.2. Совместимость

Зарубежные решения, как правило, обеспечивают лучшую совместимость с международными стандартами и другими программными продуктами.

Однако, переход на отечественные решения может обеспечить большую автономию и независимость от внешних факторов, таких как санкции.

4.3. Стоимость

Стоимость разработки и внедрения отечественного ПО, как правило, ниже в долгосрочной перспективе, однако на начальном этапе перехода могут возникнуть дополнительные затраты, связанные с обучением персонала и адаптацией процессов.

5. Рекомендации по повышению эффективности информационной безопасности

Для повышения эффективности обеспечения информационной безопасности при переходе на отечественное ПО можно рекомендовать следующие меры:

1. Провести оценку угроз и рисков с учетом специфики используемых технологий.
2. Внедрить стандарты безопасности и криптографические решения, сертифицированные в рамках национальной безопасности.
3. Регулярно проводить аудит безопасности и тестирование ПО.
4. Обеспечить обучение сотрудников и развитие системы предотвращения человеческих ошибок.
5. Разработать стратегию по обеспечению совместимости с международными стандартами безопасности и контролю за внешними угрозами.

6. Выводы

Переход на отечественное ПО в учреждениях федеральных органов исполнительной власти требует комплексного подхода к обеспечению информационной безопасности. Применение отечественных решений может повысить уровень защиты от внешних угроз и укрепить национальную безопасность, однако для обеспечения максимальной безопасности необходимо учесть риски несовершенства отечественных технологий и провести их интеграцию с международными стандартами безопасности.

7. Литература

1. Кузнецов, И. В. "Основы информационной безопасности." М.: Инфра-М, 2017.
2. Боровиков, А. В. "Защита информации в современных компьютерных системах." СПб.: БХВ-Петербург, 2020.
3. Сидоров, В. П. "Информационные технологии и их безопасность в государственном секторе." М.: Наука, 2018.
4. Шевченко, А. В. "Современные подходы к обеспечению информационной безопасности." М.: Юрайт, 2019.