Чмыхалова Анастасия Вячеславовна,
Студент Финансового университета при Правительстве РФ
Финансовый университет при правительстве РФ, Москва

Резниченко Сергей Анатольевич,
Кандидат технических наук, доцент,
доцент департамента информационной безопасности
Финансового университета при Правительстве РФ.
Финансовый университет при правительстве РФ, Москва

АНАЛИЗ РИСКОВ ИБ – ИДЕНТИФИКАЦИЯ РИСКОВ ИБ

Аннотация: Информационная безопасность (ИБ) с наше время стало неотъемлемой частью в жизнях людей, так как в современном обществе существует большое количество рисков и угроз информационным технологиям. Оценить риски и определить меры по их управлению позволяет анализ рисков ИБ. Одним из основных этапов анализа рисков ИБ - это идентификация рисков ИБ.

Ключевые слова: информационная безопасность, риски ИБ, анализ рисков ИБ, идентификация рисков ИБ.

Информационная безопасность (ИБ) становится все более важной в современном мире. Информационные технологии и Интернет предоставляют большие возможности, но их использование также подвергает пользователей рискам, связанным с разными угрозами.

Риски информационной безопасности - это возможные угрозы, которые могут повлиять на конфиденциальность, целостность или доступность информации. Они могут происходить из разных источников, включая внутренние и внешние угрозы, технические ошибки или социальную инженерию.

Рассмотрим некоторые из них:

1. Кибератаки - хакеры или злоумышленники могут успешно проникнуть в систему и получить несанкционированный доступ к конфиденциальной информации.

2. Мошенничество - самый распространенный тип угрозы, который включает в себя фишинг, фарминг и другие формы атак, цель которых выманить у пользователя конфиденциальные данные.

3. Нарушение конфиденциальности - несоблюдение политик безопасности, неправильная обработка персональных данных, утечки данных.

4. Социальная инженерия - злоумышленники могут использовать манипуляцию или обман, чтобы получить доступ к системе.

5. Непреднамеренные ошибки - сотрудники могут непреднамеренно передать конфиденциальную информацию или совершить ошибки, в результате которых может произойти утечка данных.

6. Неполадки в аппаратуре - некоторые проблемы могут произойти из-за отказа аппаратных устройств (жестких дисков, оперативной памяти, и т.д.), что может привести к утрате конфиденциальной информации.

7. Естественные катастрофы - пожары, землетрясения и другие природные катастрофы могут повлиять на конфиденциальность и доступность информации.

Все эти риски могут сильно повлиять на конфиденциальность, целостность и доступность информации и вызвать существенные финансовые потери.

Анализ рисков ИБ - это процесс идентификации, оценки и управления рисками, связанными с использованием информационных технологий в организации. Он включает в себя множество методов и инструментов, которые позволяют оценить угрозы для безопасности информации и определить меры по управлению рисками. Один из основных этапов анализа рисков ИБ - это идентификация рисков ИБ.

Идентификация рисков ИБ - это процесс определения потенциальных угроз для безопасности информации организации. Это может быть связано с нарушением конфиденциальности, целостности и доступности данных. В процессе идентификации рисков ИБ выполняются следующие действия:

1. Определение активов организации, которые нужно защитить. Это может быть информация, аппаратное обеспечение, программное обеспечение, сетевое оборудование и т.д.
2. Определение потенциальных угроз, которые могут привести к нарушению безопасности информации организации. Это могут быть кибератаки, вирусы, утечки данных, несанкционированный доступ и т.д.
3. Оценка уязвимостей системы, которые могут облегчить или усилить действие угроз. Оценка уязвимостей помогает определить, какие уязвимости существуют в системе ИБ и какую угрозу они представляют.
4. Оценка рисков, связанных с каждой потенциальной угрозой, учитывая вероятность возникновения угрозы и ее последствия.

После идентификации рисков ИБ, аналитики определяют меры по управлению рисками. Это может включать в себя рекомендации по установке дополнительных защитных мер, разработку стратегии управления рисками, обучение сотрудников и многое другое.

Важно отметить, что идентификация рисков ИБ - это не одноразовое действие. Риски ИБ могут меняться со временем, поэтому необходимы регулярные обзоры и исследования. Для этого могут использоваться такие методы, как мониторинг сетей и идентификация новых угроз, проведение тестирования на проникновение и анализ журналов событий.

В целом, анализ рисков ИБ является необходимым инструментом для организаций, который позволяет более эффективно управлять угрозами, связанными с использованием информационных систем. Идентификация рисков ИБ - это важный этап процесса анализа рисков ИБ. Она позволяет определить потенциальные угрозы, которые могут привести к нарушению

безопасности информации, и разработать меры по управлению рисками, которые помогут обеспечить безопасность информации в организации.

Список литературы:

1. Управление рисками информационной безопасности / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой.

2. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов.

3. Управление информационной безопасностью / В.В. Золотарев, Е.А. Данилова