УДК 004 **Информационные технологии**

Алиев М. И., *магистрант, ДГТУ Ростов-на-Дону, РФ*
e-mail: aliiev122@rambler.ru

АНАЛИЗ РИСКОВ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В современном цифровом мире информационная безопасность имеет первостепенное значение. С растущей зависимостью от технологий информация стала ценным активом, и необходимость ее защиты стала более острой, чем когда-либо. Важность информационной безопасности в современном цифровом мире трудно переоценить, поскольку она играет значительную роль в защите бизнеса, частных лиц и правительств от киберугроз.

Ключевые слова: информационная безопасность, киберугроза, методы управления рисками.

Abstract: In today's digital world, information security is paramount. With the growing reliance on technology, information has become a valuable asset and the need to protect it is more urgent than ever. The importance of information security in today's digital world cannot be overestimated as it plays a significant role in protecting businesses, individuals and governments from cyber threats.

Keywords: information security, cyber threat, risk management methods.

Введение

Цифровая эра привела к созданию огромных объемов данных, большая часть из которых является конфиденциальной и личной. Это включает финансовые данные, медицинские записи и другую личную информацию, которые являются ценными объектами для киберпреступников. С ростом киберпреступности защита этих данных стала главным приоритетом как для компаний, так и для частных лиц [1].

В дополнение к защите конфиденциальных данных, информационная безопасность также необходима для поддержания целостности и доступности информации. В современном цифровом мире предприятия в значительной степени полагаются на свои ИТ-системы и инфраструктуру, и любой сбой или потеря данных могут иметь серьезные последствия. Кибератаки могут привести к утечке данных, потере доходов и нанесению ущерба репутации организации. Поэтому крайне важно принимать эффективные меры безопасности для предотвращения подобных инцидентов.

Основная часть

Информационная безопасность также имеет решающее значение для защиты критически важной инфраструктуры. Это включает в себя электростанции, водоочистные сооружения и транспортные системы, которые в значительной степени зависят от ИТ-систем. Кибератака на любую из этих систем может иметь катастрофические последствия, привести к нарушению работы основных служб и даже гибели людей. Поэтому крайне важно внедрить надежные меры безопасности для защиты этих критически важных систем [2].

Наконец, информационная безопасность также необходима для защиты частной жизни отдельных лиц. С появлением социальных сетей и других онлайн-платформ люди делятся огромным количеством личной информации онлайн. Это включает в себя конфиденциальную информацию, такую как их местоположение, контактные данные и даже финансовую информацию. Эффективные меры информационной безопасности могут помочь защитить эту информацию от несанкционированного доступа и обеспечить сохранение конфиденциальности отдельных лиц.

Первым шагом в процессе оценки рисков является идентификация активов. Это включает в себя определение всех информационных активов, которые нуждаются в защите, включая аппаратное обеспечение, программное обеспечение, данные и сетевую инфраструктуру. Как только эти активы будут идентифицированы, следующим шагом будет выявление потенциальных угроз для этих активов. Это включает в себя как внутренние, так и внешние угрозы,

такие как человеческие ошибки, взлом, вредоносное ПО и стихийные бедствия [3].

После выявления потенциальных угроз следующим шагом является оценка вероятности и воздействия каждой угрозы. Это включает в себя оценку вероятности возникновения каждой угрозы и потенциальных последствий в случае ее возникновения. Эта оценка помогает расставить приоритеты в отношении рисков и определить, какие угрозы необходимо устранить в первую очередь.

После того как вероятность и воздействие каждой угрозы оценены, следующим шагом является оценка существующих средств контроля для снижения этих рисков. Это включает в себя пересмотр политик безопасности, процедур и технических средств контроля, таких как брандмауэры и средства контроля доступа. Целью этой оценки является выявление пробелов в существующих мерах безопасности и определение того, необходимы ли дополнительные меры для снижения рисков.

Заключительным шагом в процессе оценки рисков является разработка плана управления рисками. Это включает в себя разработку стратегий по снижению выявленных рисков, таких как внедрение новых мер безопасности или обновление существующих. План должен также включать график осуществления этих мер, распределение обязанностей по их осуществлению и определение ресурсов, необходимых для их осуществления.

Процесс оценки рисков - это непрерывный процесс, который следует регулярно пересматривать и обновлять по мере появления новых угроз или изменения информационных ресурсов организации. Важно обеспечить, чтобы процесс оценки рисков был всеобъемлющим, точным и тщательным, поскольку это может помочь организации снизить вероятность и воздействие потенциальных угроз.

Одной из наиболее часто используемых стратегий управления рисками является избегание рисков. Эта стратегия предполагает избегание действий или ситуаций, которые потенциально могут привести к риску. Например, если

организация работает в зоне повышенного риска, она может предпочесть избегать определенных видов деятельности в этой области, чтобы свести к минимуму риск потерь или ущерба.

Другой стратегией является снижение рисков. Это включает в себя принятие мер по снижению вероятности возникновения риска или его последствий. Например, организация может инвестировать в новые меры безопасности, чтобы снизить риск утечки данных.

Передача рисков — это еще одна стратегия, используемая в управлении рисками. Это предполагает передачу риска другой стороне, например страховой компании. Например, организация может приобрести страховку для покрытия потенциальных убытков в результате стихийного бедствия или другого события.

Удержание рисков — это стратегия, при которой организация принимает риск и его потенциальные последствия. Это может произойти, когда затраты на снижение риска превышают потенциальные потери. Например, организация может принять решение принять риск небольшой потери вместо того, чтобы инвестировать в дорогостоящие меры безопасности для ее предотвращения.

Принятие риска — это еще одна стратегия, которая предполагает принятие потенциальных рисков, связанных с деятельностью или решением. Эта стратегия часто используется, когда потенциальные выгоды от деятельности перевешивают риски. Например, организация может принять на себя риск инвестирования в новый рынок, даже несмотря на потенциальную потерю.

Существуют различные методы, используемые в управлении рисками, включая количественные и качественные методы. Количественные методы предполагают использование данных и статистического анализа для оценки рисков. Этот метод часто используется в управлении финансовыми рисками, где риски могут быть измерены в денежном выражении. Качественные методы предполагают использование экспертных суждений и субъективного анализа для оценки рисков. Этот метод часто используется в управлении нефинансовыми рисками, такими как репутационный риск.

Заключение (выводы). В заключение следует отметить, что управление

рисками является важным процессом, который помогает организациям выявлять и снижать потенциальные риски. В управлении рисками используются различные стратегии и методы, включая предотвращение рисков, снижение рисков, передачу рисков, удержание рисков и принятие рисков. Для оценки рисков используются количественные и качественные методы, в зависимости от характера риска. Внедряя эффективные стратегии управления рисками, организации могут минимизировать влияние потенциальных рисков и защитить себя от потенциальных потерь.

Так же отметим, что информационная безопасность играет решающую роль в современном цифровом мире. Это важно для защиты конфиденциальных данных, поддержания целостности и доступности информации, обеспечения соответствия нормативным требованиям, защиты критически важной инфраструктуры и защиты частной жизни отдельных лиц. По мере дальнейшего развития технологий потребность в эффективных мерах информационной безопасности будет только расти. Поэтому предприятиям, правительствам и частным лицам крайне важно уделять приоритетное внимание информационной безопасности и внедрять эффективные меры для защиты от киберугроз.

Библиографический список:

1. Галатенко, В.А. Стандарты информационной безопасности. Интернет-университет информационных технологий. ИНТУИТ.ру, 2005.

2. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008.

3. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. М.: Книжный мир, 2009.