Кириллов Максим Андреевич, студент**,**
Финансовый университет при правительстве РФ, г. Москва

Научный руководитель:
Резниченко Сергей Анатольевич, кандидат технических наук, доцент
Финансовый университет при правительстве РФ, Москва
https://orcid.org/0000-0002-1539-0457

ОСОБЕННОСТИ И ПРОБЛЕМЫ ПО ПРЕДОТВРАЩЕНИЮ ПОТВОРНОГО ВОЗНИКНОВЕНИЯ КОМПЬЮТЕРНЫХ ИНЦИДЕНТОВ

Аннотация. В современном мире компьютерные инциденты являются серьезной угрозой для бизнеса и частных лиц. Для предотвращения повторного возникновения таких инцидентов необходимо использовать современные технологии и программное обеспечение, обучать сотрудников и мониторить системы безопасности. Однако, проблемы в этой области включают сложность обеспечения безопасности распределенных систем и недостаточное знание сотрудников о правилах безопасности.

Ключевые слова:Компьютерные инциденты, безопасность, технологии, обучение, мониторинг.

Цель статьи. Обозначить особенности и проблемы, связанные с предотвращение повторного возникновения компьютерных инцидентов, предложить рекомендации по их решению

Введение

Современный мир невозможно представить без информационных технологий, которые используются во всех сферах жизни. С ростом зависимости от компьютерных систем возрастает и риск возникновения инцидентов, которые могут нанести серьезный ущерб. Поэтому

предотвращение повторного возникновения компьютерных инцидентов является одной из главных задач для компаний и организаций. Этот процесс требует особого внимания и тщательной проработки, чтобы обеспечить безопасность и надежность работы информационных систем.

В конце 2022 года «Яндекс» сообщил об утечке данных, в одном из своих сервисов, а именно, «Яндекс Еда». Несмотря на то, что платежные, банковские и регистрационные данные остались не затронутыми, в сети были опубликованы телефоны, электронные адреса и детали заказов, включая адрес доставки. В результате единичного инцидента, по компании был нанесен репутационный удар и подорвано доверие клиентов. Несложно представить какие будут последствия при повторном инциденте.

В этой статье мы разберемся в особенностях и проблемах предотвращения компьютерных инцидентов, а также, дадим несколько рекомендаций, которые помогут в предотвращении инцидентов.

Особенности предотвращения повторного возникновения компьютерных инцидентов

Компьютерные инциденты могут оказать серьезное воздействие на бизнес-процессы и безопасность организации. Поэтому, для предотвращения повторных инцидентов, необходимо активно работать над анализом причин, обучением персонала, систематическим подходом к управлению рисками и уязвимостями, обновлением и адаптацией политик и процедур безопасности, а также непрерывным мониторингом.

1. Процесс анализа причин компьютерных инцидентов. Анализ причин компьютерных инцидентов является важной составляющей предотвращения повторных инцидентов. Этот процесс включает в себя изучение причин возникновения инцидентов, выявление уязвимостей системы и причин ошибок в работе персонала. На основе полученных данных можно разработать меры, которые помогут предотвратить повторное возникновение инцидентов.

2. Обучение и подготовка персонала для предотвращения компьютерных инцидентов. Персонал – это одно из важнейших звеньев в обеспечении безопасности информации. Обучение и подготовка персонала помогут снизить вероятность возникновения инцидентов, связанных с человеческим фактором. Обучение должно включать в себя знакомство с политиками и процедурами безопасности, а также современными методами аутентификации и защиты информации.

3. Систематический подход к управлению рисками и уязвимостями. Систематический подход к управлению рисками и уязвимостями включает анализ и оценку рисков, разработку стратегии управления, реализацию мер по устранению уязвимостей и мониторинг безопасности. Это необходимо для обеспечения безопасности информационных систем и требует тщательной проработки каждого этапа и включения всех заинтересованных сторон.

4. Обновление и адаптация политик и процедур безопасности. В современном мире информационной безопасности, угрозы и риски постоянно меняются. Поэтому, регулярное обновление и адаптация политик и процедур безопасности к новым угрозам является важным элементом в предотвращении повторных инцидентов. Обновление политик должно включать в себя внедрение современных методов защиты информации, адаптацию к новым угрозам и регулярное обучение персонала.

5. Контроль доступа к данным. Контроль доступа к данным – важная составляющая информационной безопасности компании. Он позволяет управлять доступом сотрудников к конфиденциальной информации, ограничивая доступ только к необходимым данным. Важным элементом контроля доступа является ролевая система доступа. Ролевая модель – это система, в которой сотрудники имеют разные уровни доступа к данным в соответствии с их ролями и обязанностями в компании.

Таким образом, для эффективного предотвращения повторного возникновения компьютерных инцидентов необходимо систематически

подходить к управлению рисками и уязвимостями в информационных системах. Это включает процесс анализа, разработку стратегии управления, систематический подход к управлению рисками и уязвимостями, а также обновление и адаптация политик и процедур безопасности. Для достижения наилучших результатов, особенно важно проработать каждый этап и вовлечь всех заинтересованных сторон.

Проблемы предотвращения повторного возникновения компьютерных инцидентов

Предотвращение повторного возникновения компьютерных инцидентов является критически важной задачей для любой организации. Однако, на пути к достижению этой цели стоят некоторые проблемы. Рассмотрим основные проблемы, с которыми сталкиваются специалисты по информационной безопасности в процессе предотвращения повторных инцидентов.

1. Масштаб и сложность современных ИТ-систем. Современные ИТ-системы становятся все более сложными и масштабными. Это усложняет процесс обнаружения и устранения уязвимостей, а также повышает вероятность возникновения инцидентов. При этом большой масштаб систем также требует большего количества ресурсов и времени на их обслуживание и обеспечение безопасности.

2. Быстрое развитие технологий и появление новых угроз. Быстрое развитие технологий приводит к появлению новых угроз и уязвимостей. Некоторые из этих угроз могут быть очень сложными и трудно обнаруживаемыми, что усложняет процесс их предотвращения. Кроме того, развитие технологий также требует постоянного обучения и подготовки персонала организации.

3. Проблемы с обнаружением и реагированием на инциденты. Обнаружение и реагирование на инциденты является ключевой задачей в предотвращении повторного их возникновения. Не смотря на это, многие организации сталкиваются с проблемами в обнаружении инцидентов, особенно

если они происходят внутри системы, а недостаточно быстрое реагирование на инциденты может привести к серьезным последствиям, таким как утечка конфиденциальной информации или нарушение бизнес-процессов.

4. Отсутствие адекватных механизмов обмена информацией о происшествиях и угрозах. Отсутствие адекватных механизмов обмена информацией о происшествиях и угрозах между организациями является еще одной проблемой, которая может затруднить процесс предотвращения повторных инцидентов. Это может привести к тому, что другие организации не будут иметь представления об угрозах, с которыми столкнулась первоначальная организация, и не будут предпринимать меры по их предотвращению.

Решение вышеперечисленных проблем может снизить вероятность возникновения инцидентов и обеспечить безопасность информации. Поэтому, специалисты по информационной безопасности должны постоянно работать над улучшением процесса предотвращения инцидентов и развивать свои знания и навыки в этой области, чтобы успешно противостоять современным угрозам информационной безопасности.

Рекомендации по улучшению предотвращения повторного возникновения компьютерных инцидентов

Уже были рассмотрели основные проблемы и особенности, с которыми сталкиваются специалисты по информационной безопасности в процессе предотвращения повторных компьютерных инцидентов. Сейчас же стоит рассмотреть несколько рекомендаций, которые могут помочь улучшить стратегию предотвращения инцидентов.

Одним из наиболее важных факторов, который может помочь улучшить стратегию – это «Усиление межотраслевого и международного сотрудничества в области информационной безопасности». Совместная работа может помочь лучше понимать угрозы, а обмен информацией о происшествиях и угрозах может помочь организациям более эффективно реагировать на инциденты и

предотвращать их повторное возникновение. Кроме того, сотрудничество может помочь организациям лучше понимать новые угрозы и адаптироваться к изменяющейся ситуации.

Одной из основных проблем в предотвращении компьютерных инцидентов является ограниченный доступ к современным инструментам и технологиям, которые могут помочь в обнаружении и предотвращении угроз. Инвестирование в специализированные инструменты и технологии может помочь организации повысить свою защиту и обеспечить более быстрое и эффективное реагирование на инциденты. Решения в этой области могут варьироваться от системы мониторинга событий до систем управления уязвимостями и автоматизированных инструментов поиска угроз.

Выше, я писал о том, что важно привлекать всех заинтересованных сторон. Из этого вытекает следующая рекомендация по улучшению предотвращения повторного возникновения компьютерных инцидентов «Повышение осведомленности и поддержки со стороны руководства организаций». Повышение осведомленности и поддержки со стороны руководства организаций может помочь в обеспечении эффективной стратегии предотвращения инцидентов. Руководство должно понимать, что информационная безопасность является критически важным аспектом бизнеса и должна получать соответствующее внимание и ресурсы. Кроме того, руководство должно активно поддерживать меры по обеспечению безопасности и поощрять сотрудников принимать активное участие в процессе предотвращения инцидентов.

Заключение

В заключении данной статьи можно отметить, что предотвращение повторного возникновения компьютерных инцидентов является одной из основных задач, стоящих перед специалистами по информационной безопасности. Несмотря на то, что существует множество инструментов и методов для предотвращения инцидентов, все еще существуют ряд проблем,

которые могут затруднять процесс их предотвращения. Для решения этих проблем необходимо инвестировать в специализированные инструменты и технологии для обнаружения, анализа и предотвращения инцидентов. Кроме того, усиление межотраслевого и международного сотрудничества в области информационной безопасности может помочь организациям лучше понимать угрозы и совместно работать для их предотвращения. Наконец, повышение осведомленности и поддержки со стороны руководства организаций может помочь в обеспечении эффективной стратегии предотвращения инцидентов.

В целом, предотвращение повторного возникновения компьютерных инцидентов является сложной задачей, но с помощью правильных инструментов, сотрудничества и поддержки со стороны руководства, организации могут снизить вероятность возникновения инцидентов и обеспечить безопасность своей информации.

Список литературы:

1. Ю.А. Гатчин, Е. В. Климова (2011) «ВВЕДЕНИЕ В КОМПЛЕКСНУЮ ЗАЩИТУ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ»

2. А. Ю. Щеглов (2014) «МОДЕЛИ, МЕТОДЫ И СРЕДСТВА КОНТРОЛЯ ДОСТУПА К РЕСУРСАМ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ».

3. Нилуфархон Эркинходжаевна Курбановна (2021) «МЕТОДЫ ПРЕДОТВРАЩЕНИЯ УГРОЗ КИБЕРБЕЗОПАСНОСТИ»

4. Управление информационной безопасностью. [Электронный ресурс]. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/upravlenie-informatsionnoj-bezopasnostyu/