Антюфьева Анастасия Валерьевна, студентка,
Финансовый университет при правительстве РФ,
г. Москва

Каракич Антон Алексеевич, студент,
Финансовый университет при правительстве РФ,
г. Москва

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

# ОСОБЕННОСТИ И ПРОБЛЕМЫ ПРЕДОТВРАЩЕНИЯ ПОВТОРНОГО ВОЗНИКНОВЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Аннотация.** Главными направлениями работы для предотвращения возникновения повторных инцидентов являются обучение персонала, введение политики безопасности и регулярное обновление систем. Часто причинами повторного появления инцидента становятся несоблюдение правил и норм, недостаточные ресурсы, отсутствие системного анализа событий и неправильная оценка рисков.

**Ключевые слова:** информационная безопасность, компьютерная безопасность, компьютерный инцидент, инцидент информационной безопасности, предотвращение инцидентов.

## 1. Что из себя представляет компьютерный инцидент и с чем он связан?

Компьютерный инцидент – ситуация с несоблюдением или прекращением функционирования объекта информационной инфраструктуры, применяемой для организации взаимодействия или несоблюдения безопасности, обрабатываемой таким объектом информации, в том числе случившийся в результате компьютерной атаки.

В России существует стандарт ГОСТ Р ИСО/МЭК 27001– 2006. В нем содержатся требования, которые связанны с управлением инцидентами ИБ. Инцидент информационной безопасности– возникновение одного или нескольких событий ИБ, которые могут причинить ущерб активам организации. Инциденты ИБ можно поделить на преднамеренные (преднамеренное несоблюдение политики безопасности) или случайные (могут быть вызваны непредумышленной человеческой ошибкой), еще их можно поделить на технические средства (компьютерные вирусы) и нетехнические (кража компьютеров).

Появление инцидентов ИБ может быть связано с:

– невозможность систем функционировать с исходной продуктивностью (при полном отказе в доступе авторизованным пользователям);

– действиями, которые связанны с определением вероятных целей атаки и получением представления о сервисах, функционирующих на идентифицированных задачах атаки;

– несанкционированных попыток доступа в систему или ошибочного использования системы, сервиса или сети.

ГОСТ Р ИСО/МЭК 27001–2006 характеризует инцидент ИБ как любое незапланированное или неблагоприятное событие, которое может разрушить деятельность или информационную безопасность.

В роли инцидентов информационной безопасности приводятся некоторые события:

− потеря устройств или оборудования;

− системные сбои;

− ошибки пользователей;

− игнорирование и несоблюдение политики;

− несоблюдение физических мер защиты;

− несоблюдение правил доступа.

Процесс управления инцидентами ИБ можно поделить на 5 этапов:

1. планирование и организация;

2. выявление;

3. оценка и принятие;

4. принятие ответных мер;

5. извлечение уроков.

Реагировать на инцидент нужно в зависимости от масштаба ущерба и серьезности нарушения.

Сперва организации нужно подготовиться к реагированию на инцидент. Первый этап подготовки заключается в разработке политик и планирование самой деятельности по управлению инцидентами и нужно сформировать группу реагирования на инциденты.

Далее, персонал проходит обучение и вводятся нужные технические меры (например, резервное копирование). Выявление событий ИБ происходит за счет: первое это сбора информации об уязвимостях безопасности путем анализа систем и мониторинга на отсутствие угроз и уязвимостей. После информация, которая связанна с возникновением событий ИБ, оценивается. Затем принимается решение, считаются ли эти события инцидентами ИБ.

Далее нужно выяснить, какие части были затронуты в информационной инфраструктуре. Возможно придется отключать пораженные системы, смену паролей и т.д. Потом нужно устранить элементы инцидента (удалить

вредоносные программы, отключить взломанные учетные записи пользователей).

Так же может потребоваться восстановить систему до работоспособного состояния, и восстановить данные из резервных копий. Достаточно значимым рассматривается деятельность после закрытия инцидента, она состоит из извлечения уроков из случившегося для избежания похожих случаев в будущем. То есть это увеличивает эффективность реагирования, тем самым совершенствует деятельность по управлению инцидентами ИБ.

## 2. Средства обнаружения инцидентов ИБ.

Обнаружение инцидентов:

− инциденты могут быть выявлены разными методами, с различными показателями достоверности, так же, могут быть ошибочные срабатывания автоматизированных систем обнаружения;

− некоторые инциденты имеют очевидные признаки, которые легко заметить, но большинство других инцидентов практически нельзя найти, так как они не имеют похожих признаков;

− Происшествия ИБ, которые действительно могут являться признаками инцидентов ИБ большой, но не все они могут свидетельствовать о вправду случившихся инцидентах ИБ (сбой сервера может случиться по некоторым причинам, они могут быть отличными от инцидента ИБ, в том числе могут включать человеческую ошибку);

− Для идентификации событий инцидента ИБ могут понадобиться особые технические знания, информация о самом инциденте может быть получена от различных систем и записана в нескольких журналах, каждый из них может отображать какую-либо часть данных об инциденте.

При оценке событий безопасности и идентификации инцидента нужно исходить из неоднозначных сведений, чтобы определить, что именно произошло.

### 3. Первичное реагирование на инцидент ИБ.

В основном на раннем этапе реагирования на инцидент ИБ сложно определить, что послужило его причиной и будут ли собранные доказательства инцидента объектом исследования в рамках расследования.

Основная задача реагирования на инцидент это - обеспечение целостности важных сведений для их исследования в будущем. Группа реагирования на инциденты должна следить, чтобы цифровые доказательства находились в надежном месте, и чтобы это контролировалось.

При осуществлении исследовании копии содержимого сетевого трафика и оперативной памяти могут применяться для выявления следов работы вредоносных программ и следов активности нарушителя.

Также нужно копировать файлы самого сетевого оснащения путем передачи некоторых типов данных, такие как журналы доступа и журналы сетевых событий из интерфейса управления устройством на съемный носитель.

Организовываются мероприятия. Они могут содержать в себе информирование руководства данной организации и подразделений ИБ о самом факте инцидента. Так же документы, которые были разработаны при проведении мероприятий, могут являться доказательствами для изучения вопросов, выносимых на разрешение при назначении судебных экспертиз носителей информации организации.

Что нужно сделать при нарушениях ИБ:

1. Убедиться, что инцидент действительно есть.

2. Устранить область ИТ-инфраструктуры, которая была задействована в инциденте.

3. Нужно ограничить допуск объектам, которые были использованы в инциденте.

4. Написать служебную записку на имя директора организации о появлении инцидента.

5. Проконсультироваться с экспертами.

6. Составить план по сбору доказательств об инциденте и собрать группу по расследованию инцидента.

7. Организовать целостность доказательств.

8. В присутствии независимой стороны извлечь и опечатать носители информации с доказательной базой.

9. После составления доказательств восстановить работоспособность информационных систем.

10. Во время изучения источников информации гарантировать неизменность доказательств (работать только с копией).

11. В конце расследования написать отчет и предложить инструкции, чтобы снизить риски появления похожих инцидентов в будущем.

## 4. Сбор свидетельств инцидента ИБ.

Чтобы собрать свидетельства инцидента нужно обеспечить:

- Чтобы из полученных свидетельств можно было извлечь ценную информацию, чтобы содействовать расследованию конкретного инцидента;

- Чтобы собранные свидетельства были достаточны для объективного суждения об инциденте;

- Чтобы свидетельства были получены из доверенных источников и неизменны;

- Чтобы свидетельства были получены легальным способом.

## 5. Особенности предотвращения повторного возникновения компьютерных инцидентов.

1. Анализ инцидента. Каждый инцидент должен быть подробно проанализирован, чтобы определить точные причины его возникновения.

2. Исправление уязвимостей. Для того чтобы избежать будущих инцидентов, необходимо устранять уязвимости, которые могут привести к нарушению безопасности.

3. Создание конкретных правил безопасности. Компания должна создать четкие правила безопасности, которые должны быть соблюдены всеми сотрудниками.

4. Обучение сотрудников. Каждый сотрудник должен быть обучен правилам безопасности информации и процедурам, необходимым для работы в безопасной среде.

## 6. Проблемы предотвращения повторного возникновения компьютерных инцидентов.

1. Недостаточная информация о возможных угрозах и уязвимостях.

2. Отсутствие контроля и мониторинга за инцидентами.

3. Недостаток средств для реагирования на инциденты.

4. Невозможность или сложность обновления и модернизации систем безопасности.

## 7. Особенности предотвращения повторных компьютерных инцидентов.

1. Обучение персонала - Один из главных факторов - это повышение квалификации персонала. Информационная безопасность должна быть основным приоритетом в обучении сотрудников.

2. Введение политики безопасности - Существует необходимость установления строгих правил и правил этики для обработки и защиты конфиденциальной информации.

3. Регулярное обновление систем - регулярное обновление операционной системы, приложений и антивирусного программного обеспечения поможет избежать многих уязвимостей, которые могут быть использованы злоумышленниками.

Некоторые из проблем, которые возникают при предотвращении повторных компьютерных инцидентов, включают в себя:

1. Несоблюдение правил и норм - несмотря на обучение и установку политики безопасности, некоторые люди могут не следовать правилам, что может подвергнуть организацию риску нарушения конфиденциальности.

2. Низкие бюджетные ограничения - Информационная безопасность может быть дорогостоящей, и при ограниченном бюджете организаций может быть сложно обеспечить достаточную защиту.

3. Создание новых уязвимостей - при обновлении систем и программного обеспечения новые уязвимости могут появляться и могут быть использованы злоумышленниками. Поэтому такие обновления нужно выполнять с осторожностью.

4. Анализ событий. После того, как был обнаружен инцидент, следует провести анализ событий, чтобы выяснить, каким образом он произошел. Это поможет выявить уязвимости в системе и принять меры по их устранению.

5. Улучшение системы безопасности. После проведения анализа событий можно принимать меры по улучшению системы безопасности, которые были обнаружены в результате анализа. Например, можно обновить программное обеспечение, установить новые антивирусные программы, улучшить механизмы контроля доступа и т.д.

6. Обучение персонала. Часто причина инцидента связана с неправильными действиями пользователей. Поэтому необходимо проводить обучение сотрудников по правилам безопасности, протоколам работы и поведению в случае возникновения инцидента.

7. Недостаточные ресурсы. Проведение анализа событий и улучшение системы безопасности требуют больших затрат времени и ресурсов.

8. Недостаток экспертов. Удаление уязвимостей и улучшение системы безопасности требуют опыта и знаний в области информационной безопасности. Нередко компаниям не хватает экспертов в этой области.

9. Неправильная оценка рисков. Часто компании не учитывают возможные риски, связанные с нарушением безопасности. Поэтому необходимо учитывать

все возможные сценарии и не допускать стихийных ситуаций, которые могут привести к инцидентам.

*Список литературы:*

1. https://www.smart-soft.ru/blog/information-security-incident-investigation/

2. https://ir.alfastrah.ru/posts/629