Шаханова М.В., Четверик М.А., Шаханова В.С. Защита информации в условиях чрезвычайных ситуаций // Международный журнал информационных технологий и энергоэффективности. – 2024. –Т. 9 № 12(50) с. 96–101

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЗАЩИТА ИНФОРМАЦИИ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

[1]Шаханова М.В., Четверик М.А., Шаханова В.С.
ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: [1]marinavl2007@yandex.ru

Защита информации в условиях чрезвычайных ситуаций представляет собой важную тему, которая охватывает множество аспектов, включая правовые, технические и организационные меры. Чрезвычайные ситуации, вызванные природными катастрофами и техногенными авариями, создают угрозу как для физической безопасности, так и для информационной инфраструктуры. В моменты опасности, данные и системы, обеспечивающие функционирование организаций и государственных структур, наиболее подвержены повреждению. Эффективная защита информации в условиях ЧС требует комплексного подхода, включающего не только анализ потенциальных угроз, уязвимостей и способы предотвращения потерь, но также методы защиты, не допускающие эти самые потери.

Ключевые слова: Чрезвычайная ситуация, угрозы, защита информации, информационные инфраструктуры, организации, методы защиты.

INFORMATION PROTECTION IN EMERGENCY SITUATIONS

[1]Shakhanova M. V., Chetverik M.A., Shakhanova V.S.
MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: [1]marinavl2007@yandex.ru

Information protection in emergency situations is an important topic that covers many aspects, including legal, technical and organizational measures. Emergencies caused by natural disasters and man-made accidents pose a threat to both physical security and information infrastructure. In times of danger, the data and systems that ensure the functioning of organizations and government structures are most susceptible to damage. Effective protection of information in an emergency requires an integrated approach that includes not only analysis of potential threats, vulnerabilities and ways to prevent losses, but also protection methods that prevent these very losses.

Keywords: Emergency, threats, information protection, information infrastructures, organizations, protection methods.

Чрезвычайные ситуации. Угрозы и Уязвимости

Чрезвычайная ситуация (ЧС) - обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде, значительные материальные потери и нарушение условий жизнедеятельности людей. [1]

В условиях ЧС существует реальная угроза для защиты информации, что может привести к серьезным последствиям как для отдельных организаций, так и для национальной безопасности. Чрезвычайные ситуации могут вызвать разрушение инфраструктуры, включая

системы, отвечающие за хранение и обработку данных. В таких ситуациях организации рискуют потерять не только данные, но и доверие клиентов, партнеров и регуляторов.

Исходя из всего выше перечисленного, можно сформулировать потенциальные угрозы, которые могут коснуться информационных систем и повлиять на их функциональность в условиях чрезвычайных ситуациях.

Потенциальные угрозы:

1. Природные катастрофы
- Ураганы и торнадо: могут вызвать повреждение физической инфраструктуры и оборудования.
- Землетрясения: способны вызвать разрушение зданий и систем хранения данных.
- Наводнения: могут затопить серверные комнаты и офисы.
2. Техногенные аварии
- Пожары, утечки химических веществ.
- Поломка оборудования, сбои на сетях электроснабжения: приводит к отключению систем.
3. Кибератаки
- Кибератаки, атаки на инфраструктуру (DDoS, SQL-инъекции).
- Вредоносное ПО.
4. Человеческий фактор
- Ошибки сотрудников.
- Недостаточная осведомленность сотрудников.
- Умышленное или неумышленное раскрытие данных.
5. Террористические акты
- Уничтожение физической инфраструктуры.
- Кибератаки на критически важные системы.

Кроме физического разрушения, ЧС могут существенно ослабить или вовсе подорвать безопасность информационных систем. В хаотичной обстановке возрастает вероятность кибератак, когда злоумышленники могут воспользоваться ситуацией, чтобы получить доступ к системам, которые становятся менее защищенными. Поскольку внимание сотрудников и служб безопасности часто сосредоточено на разрешение текущих проблем, шанс на успешную кибератаку значительно увеличивается.

Уязвимости, возникающие при чрезвычайных ситуациях, могут возникать из-за повреждений оборудования, снижения качества обслуживания и человеческих ошибок. Рассмотрим наиболее критические из них:

1. Недостаточная защита данных
- Отсутствие шифрования и контроля доступа.
- Слабые пароли и их частая смена.
2. Системные уязвимости
- Отсутствие обновлений безопасности.
- Уязвимости в устаревших приложениях и ПО.
- Неправильные настройки, неверные конфигурации.
3. Отсутствие резервного копирования

- Неправильные или отсутствующие процедуры резервного копирования данных, как правило, в последующем, невозможность восстановления после утраты данных.

4. Неподготовленность персонала

- Недостаточная осведомленность о методах защиты информации.
- Отсутствие тренингов по действиям в условиях ЧС.
- Неполные или неэффективные процедуры реагирования на инциденты.
- Нехватка ресурсов для обеспечения безопасности.

Чрезвычайные ситуации могут возникнуть в любой момент, и не всегда люди и организации будут готовы к этому. Поэтому основной задачей в области защиты информации в условиях ЧС является не восстановление данных и поврежденного оборудования после происшествия, а минимизация или полное предотвращение нарушения работы оборудования в чрезвычайных условиях.

Это подчеркивает важность разработки комплексного подхода к защите информации, который учитывал бы риски, возникающие в условиях нестабильной обстановки, и указывал бы на методы повышения устойчивости информационных систем.

Законодательство и нормативные акты по защите информации в условиях ЧС

Существует множество законов и стандартов, регулирующих защиту информации в условиях чрезвычайных ситуаций. Эти документы определяют правовые рамки, обязательства и меры, которые должны принимать организации для обеспечения безопасности информации и минимизации последствий ЧС. Рассмотрим основные аспекты законодательства и нормативных актов:

1. Законодательные инициативы

В большинстве стран существуют специальные законы, касающиеся защиты информации и данных. К ним относятся законы о защите персональных данных, такие как Общий регламент по защите данных (GDPR) в Европейском Союзе и Закон о защите персональной информации (CIPA) в США. В России законом, регулирующим любые действия, связанные с информацией, выступает Федеральный закон "Об информации, информационных технологиях и о защите информации". Эти законы устанавливают требования относительно обработки, хранения и защиты данных, а также обязывают организации уведомлять пользователей о возможных утечках данных, что становится особенно актуальным в условиях ЧС. [4]

2. Нормативные акты по безопасности информации

На уровне национальных и международных стандартов разрабатываются нормативные акты, которые направлены на установление лучших практик в области информационной безопасности. Например:

- ISO/IEC 27001 — международный стандарт, который описывает требования к системам управления информационной безопасностью (СУИБ). Он включает рекомендации по идентификации и оценке рисков, что особенно актуально в условиях ЧС. [2]
- NIST SP 800-53 — набор рекомендаций от Национального института стандартов и технологий США, который предоставляет контрольные механизмы для управления рисками и защиты информации. [5]

Эти стандарты обеспечивают структуру для разработки внутренних политик и процедур, направленных на защиту информации и минимизацию потенциального ущерба.

3. Подготовка и реагирование на ЧС

Также имеются документы, описывающие порядок действий в случае возникновения ЧС. Например, в России действует Федеральный закон «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», который определяет меру государственного реагирования на ЧС, включая обязательные требования для организаций по подготовке планов по защите информации.

Организации обязаны разрабатывать и внедрять планы реагирования на ЧС, которые включают процедуры по обеспечению устойчивости информационных систем, а также механизмов оперативного восстановления после инцидентов. Это включает в себя регулярные тренировки и учения, что позволяет поддерживать готовность и отрабатывать навыки реагирования. [3]

Методы предотвращения сбоев в информационных системах при ЧС

Обеспечение устойчивости информационных систем в условиях чрезвычайных ситуаций является критически важной задачей для организаций. Эффективные меры предосторожности позволяют минимизировать риски, связанные с потерей данных и нарушениями функционирования систем. Рассмотрим ключевые методы, которые можно использовать для предотвращения сбоев.

1. Разработка и внедрение планов реагирования

Первым шагом к предотвращению сбоя является создание детализированных планов реагирования на ЧС. Эти планы должны включать сценарии различных типов ЧС и четкие инструкции по действиям сотрудников. Необходимо определить ответственных лиц и создать рабочие группы, способные оперативно реагировать на угрозы. Регулярные тренировки помогут сотрудникам отработать действия в условиях стресса и недостачи ресурсов.

2. Обеспечение резервного копирования

Регулярное резервное копирование данных является основным компонентом защиты информации. Данные должны копироваться как на локальные устройства, так и в облачные хранилища, чтобы обеспечить доступ к ним в случае повреждения основной системы. Важно также тестировать процессы восстановления, чтобы убедиться, что в случае необходимости данные могут быть быстро восстановлены.

3. Использование технологий высокой доступности

Технологии высокой доступности позволяют минимизировать время простоя систем и обеспечить непрерывность бизнеса. Это может осуществляться с помощью кластеризации серверов, дублирования критически важных компонентов и использования географически распределенных дата-центров. Такие меры позволяют снизить вероятность полного отключения сервисов при возникновении ЧС.

4. Обучение сотрудников

Поддержание уровня осведомленности сотрудников о безопасности информации является важным аспектом предотвращения сбоев. Регулярные тренинги по вопросам безопасности, включая фишинг и другие киберугрозы, помогут предотвратить человеческие ошибки, которые могут привести к утечкам или повреждению данных.

5. Проведение регулярной оценки рисков

Организации должны регулярно проводить оценку рисков, связанных с защитой информации. Это включает в себя анализ потенциальных угроз и уязвимостей, а также определение возможности возникновения ЧС. На основе результатов такой оценки можно корректировать свои стратегии и планы реагирования, делая их более эффективными.

Применение этих методов способствует созданию безопасной и устойчивой инфраструктуры, что имеет решающее значение для обеспечения защиты информации в условиях нестабильной обстановки.

Заключение

Защита информации в условиях чрезвычайных ситуаций требует комплексного подхода, который основывается на тщательной оценке рисков и анализе угроз. Организации, осознающие риски и занимающиеся проактивной подготовкой к возможным инцидентам, способны значительно снизить вероятность потерь и сохранить свою репутацию. Внедрение эффективных планов реагирования, регулярное обучение сотрудников и взаимодействие с государственными структурами — ключевые элементы, позволяющие организациям адаптироваться и успешно действовать в изменчивой и неустойчивой обстановке.

Список литературы

1. Государственный стандарт РФ. Безопасность в чрезвычайных ситуациях. Термины и определения основных понятий / авт. Всероссийский научно-исследовательский институт по проблемам ГО и ЧС с участием рабочей группы специалистов Технического комитета по стандартизации ТК 71 “Гражданская оборона, предупреждение и ликвидация чрезвычайных. - 1996 г.. - (ноябрь 2000 г.) с Изменением N 1, принятым в мае 2000 г. (ИУС N 8-2000).
2. Международный стандарт ISO/IEC 27001:2022. - 2022 г.. - Издание 3 .
3. Федеральный закон о защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера [В Интернете]. - 11 ноябрь 1994 г.. - https://www.consultant.ru/document/cons_doc_LAW_5295/.
4. Федеральный закон об информации, информационных технологиях и о защите информации [В Интернете]. - 8 июль 2006 г.. - https://www.consultant.ru/document/cons_doc_LAW_61798/.
5. Security and Privacy Controlsfor [В Интернете] / авт. FORCE JOINT TASK // Security and Privacy Controlsfor. - Sep 2020 г.. - NIST Special Publication 800-53 Revision 5. - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

References

1. The state standard of the Russian Federation. Safety in emergency situations. Terms and definitions of basic concepts / author. All-Russian Research Institute on Civil Defense and Emergency Situations with the participation of a working group of specialists of the Technical Committee for Standardization TC 71 “Civil Defense, prevention and liquidation of emergencies. - 1996. - (November 2000) with Amendment No. 1, adopted in May 2000 (IUS No. 8-2000).
2. International standard ISO/IEC 27001:2022. - 2022. - Edition 3 .

3. The Federal Law on the Protection of the Population and Territories from Natural and Man-made Emergencies [On the Internet]. - November 11, 1994. - https://www.consultant.ru/document/cons_doc_LAW_5295 /.
4. Federal Law on Information, Information Technologies and Information Protection [On the Internet]. - July 8, 2006. - https://www.consultant.ru/document/cons_doc_LAW_61798 /.
5. Security and Privacy Controlsfor [On the Internet] / auth. FORCE JOINT TASK // Security and Privacy Controlsfor. - Sep 2020. - NIST Special Publication 800-53 Revision 5. - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.