КИБЕРБЕЗОПАСНОСТЬ В ЭКОЛОГИЧЕСКИХ ПРОЕКТАХ: УГРОЗЫ И ЗАЩИТА ИНФОРМАЦИИ

Федоркина И.А., к.э.н., доцент,

Минеев Н.С. студент

МТУСИ, г. Москва, Россия

Аннотация. Проблема информационной безопасности является одним из актуальных вопросов, стоящих в век цифровизации данных. В статье рассказано о методах атак и защиты, которые применяются в современном технологическом мире.

Ключевые слова: информационная безопасность, экологические исследования, защита информации.

Технологии «больших данных» в начале века во многом изменили ландшафт и архитектуру современных информационных систем[1]. Кибербезопасность становится все более актуальной и важной областью в современном мире, особенно в контексте экологических проектов. Экологические проекты часто включают в себя сбор и обработку больших объемов данных о природных ресурсах, использование современных технологий для мониторинга окружающей среды и защиты экосистем.

Однако, вместе с ростом цифровизации и автоматизации в этой области, возникают новые угрозы для безопасности информации и технологических систем. Безопасность современных цифровых сервисов напрямую зависит, в том числе, и от безопасности обрабатываемых в них данных, которые не только используются для предоставления сервиса или получения результата, услуги, но и для создания и функциональности самих цифровых решений [1].

Проблема кибербезопасности в экологических проектах становится особенно актуальной в свете потенциальных последствий кибератак на инфраструктуру, обработку и анализ данных, а также на саму экосистему. Для работы с климатическими данными широко применяются информационные технологии, которые позволяют собирать, систематизировать, анализировать, проводить предварительные расчёты, визуализируют данные [2].

Уязвимости в системах мониторинга и контроля могут привести к неправильным оценкам состояния окружающей среды и неправильным решениям в области охраны природы. Кроме того, утечка конфиденциальной информации о природных ресурсах может негативно отразиться на стратегиях управления природными ресурсами и привести к экологическим катастрофам.

К примеру, экологические проекты часто собирают и анализируют большие объемы данных о состоянии окружающей среды, включая информацию о биоразнообразии, климатических изменениях, и других важных факторах. Эта информация может содержать конфиденциальные данные о местоположении редких видов, уязвимости экосистем и даже охраняемых территориях. Защита конфиденциальности этих данных

необходима для предотвращения нежелательного доступа и неправомерного использования.

Искаженные данные могут привести к неправильным выводам о состоянии окружающей среды и способах её охраны. Кибератаки могут нарушить целостность данных, что создаст риск неправильных оценок и решений, влияющих на экологическую политику и практику.

Экологические проекты, особенно те, которые зависят от сетевых и информационных технологий для сбора и анализа данных, могут быть подвержены прерываниям в случае кибератак или других нарушений безопасности. Защита информации помогает обеспечить непрерывность проектов и предотвращает их прекращение из-за технических сбоев.

Экологические проекты часто зависят от поддержки общественности и сотрудничества с различными партнёрами, включая правительственные организации, неправительственные организации и частные компании. Утечка данных или нарушения безопасности могут подорвать доверие общественности и сотрудничество с партнёрами, что может серьёзно затруднить выполнение проектов и достижение их целей.

Атаки на системы мониторинга и контроля окружающей среды представляют серьезную угрозу для экологических проектов и окружающей среды в целом.

Например, внедрение вредоносного программного обеспечения (malware). Злоумышленники могут внедрять вредоносное ПО в системы мониторинга и контроля, что позволяет им получать несанкционированный доступ к данным или даже принимать управление над устройствами. Это может привести к искажению данных или прекращению работы систем, что может повлечь за собой неправильные выводы о состоянии окружающей среды и неправильные решения в области её охраны.

Также возможны атаки отказом в обслуживании (DDoS). Злоумышленники могут осуществлять DDoS-атаки на серверы систем мониторинга и контроля, перегружая их запросами и тем самым приводя к временным простоям или даже полной недоступности систем. Это может привести к потере данных и непрерывности мониторинга, что снизит эффективность экологических проектов и может создать реальные угрозы для окружающей среды.

Не стоит забывать и про физические атаки на устройства и инфраструктуру. Нападение на физическую инфраструктуру систем мониторинга и контроля, такие как датчики, приборы сбора данных или коммуникационные сети, может привести к их повреждению или уничтожению. Это может остановить процесс сбора данных и мониторинга, что создаст пробелы в информации о состоянии окружающей среды и затруднит принятие необходимых мер по её охране.

А также, перехват и подмена данных. Злоумышленники могут перехватывать передаваемые данные между датчиками и серверами или же подменять их на ложные. Это может привести к искажению данных и введению в заблуждение аналитиков и принимающих решения, что может повлечь за собой неправильные действия по охране окружающей среды.

Ключевым аспектом обеспечения кибербезопасности в проектах по охране труда являются разработка и внедрение сетевых защитных механизмов. Для защиты сетевой инфраструктуры экологических проектов применяются такие шаги, как анализ угроз и уязвимостей
сетевой инфраструктуры,
установка межсетевых экранов, которые
помогают фильтровать трафик между различными сегментами сети, контролируя доступ к ресурсам и блокируя подозрительную активность. Также, для защиты применяются
системы обнаружения вторжений (IDS) и предотвращения вторжений (IPS)
созданные для обнаружения аномальной активности в сети и автоматического реагирования на потенциальные угрозы, блокируя или изолируя подозрительные устройства или пользователей[3]. Во многих системах обязательным является ш ифрование трафика
между устройствами в сети. Оно помогает защитить данные от перехвата и подмены злоумышленниками. Применение протоколов шифрования, таких как SSL/TLS, обеспечивает конфиденциальность передаваемой информации.

Роль кибербезопасности в обеспечении эффективности и устойчивости экологических проектов оказывается критически важной в наше время. Экологические проекты сегодня основываются на использовании современных информационных технологий и цифровых инструментов для сбора, анализа и управления данными о состоянии окружающей среды. Однако, рост зависимости от цифровых технологий также увеличивает уязвимость проектов к кибератакам и другим угрозам безопасности.

Кибербезопасность играет ключевую роль в защите конфиденциальности данных, обеспечении целостности информации, сохранении непрерывности проектов и поддержании доверия общественности и партнёров. Успешное внедрение сетевых защитных механизмов, создание планов реагирования на кибератаки и обучение персонала по основам кибербезопасности помогает минимизировать риски и повышает устойчивость экологических проектов перед современными угрозами.

Для достижения своих целей экологические проекты должны интегрировать кибербезопасность в свою общую стратегию безопасности и управления рисками. Только таким образом можно обеспечить эффективную защиту информации, сохранение ценных данных о природных ресурсах и успешную реализацию проектов по охране окружающей среды в будущем.

Значимость дальнейших исследований в области кибербезопасности для экологического сообщества необходимо подчеркнуть, учитывая быстрое развитие технологий и возрастающие угрозы в сфере кибербезопасности.

Одним из ключевых аспектов является идентификация новых угроз. С развитием технологий появляются новые уязвимости и угрозы для экологических проектов. Непрерывное исследование современных методов атак и уязвимостей поможет эффективно защитить проекты от новых угроз.

Другим ключевым аспектом можно назвать разработку новых методов защиты. Дальнейшие исследования позволят разработать более продвинутые методы защиты информации в экологических проектах, включая разработку новых технологий шифрования, методов обнаружения аномального поведения и т. д.

Нельзя не упомянуть про оценку рисков и уязвимостей. Дальнейшие исследования позволят более глубоко понять риски и уязвимости, связанные с использованием цифровых технологий в экологических проектах, что поможет разработать более эффективные стратегии обеспечения безопасности.

И, наконец, анализ последствий кибератак. Исследования позволят лучше понять последствия кибератак на экологические проекты, включая их влияние на среду, общественное доверие и результаты проектов. Это поможет разработать более эффективные методы реагирования на инциденты.

В заключении, необходимость принятия мер для защиты информации в экологических проектах неоспорима. Современные экологические проекты сталкиваются с растущей угрозой кибератак и других киберугроз, которые могут нанести серьезный ущерб как окружающей среде, так и проектам сами по себе. Защита конфиденциальности данных, обеспечение целостности информации и обеспечение непрерывности проектов становятся приоритетом в условиях современной цифровой эры.

Только путем эффективной защиты информации и реализации современных мер безопасности информации экологические проекты могут обеспечить свою устойчивость, надежность и успешное выполнение своих целей. Необходимо стремиться к интеграции кибербезопасности во все аспекты планирования, реализации и управления экологическими проектами, чтобы минимизировать риски и гарантировать сохранение природных ресурсов для будущих поколений.

Литература

1. Полтавцева, М. А. Многоуровневая концепция безопасности систем управления большими данными / М.А. Полтавцева, Д.П. Зегжда, М.О. Калинин // Вопросы кибербезопасности. – 2023. – № 5(57). – С. 25-36. – DOI 10.21681/2311-3456-2023-5-25-36. – EDN KDMIMW.

2. Гусельников, Г.М. Применение информационных технологий для сбора климатических данных с метеорологических станций австралии / Г.М. Гусельников, В.Д. Ананьев, Ж.С. Жукова // Актуальные проблемы техносферной безопасности: Сборник научных трудов V Международной научно-практической конференции студентов, аспирантов, молодых ученых, преподавателей, Ульяновск, 17–20 мая 2023 года. – Ульяновск: Ульяновский государственный технический университет, 2023. – С. 18-22. – EDN NXIRTD.

3. Родивилин, И.П. Социальная инженерия как угроза информационной безопасности: тенденции и защита / И.П. Родивилин // Информационные технологии и математическое моделирование в управлении сложными системами. – 2023. – № 3(19). – С. 30-38. – EDN GXPRNK.