МЕТОДИКА ОЦЕНКИ ЭКОЛОГИЧЕСКОЙ ЗНАЧИМОСТИ УГРОЗ ОБЪЕКТУ КИИ НА ПРИМЕРЕ ОБЪЕКТА АСУ ТП

В.С. Деревянко, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, vladimirderevyanko@bk.ru.*

УДК 004.056.5

Аннотация. В современном мире все чаще происходят атаки на автоматизированные системы управления, в том числе на объекты критической информационной инфраструктуры. Успешные вредоносные вмешательства могут приводить к негативным последствиям. Для того, чтобы этого избежать, необходимо строго соблюдать требования и правила категорирования объектов КИИ, а также обеспечивать безопасность функционирования систем управления, в том числе экологической.

Ключевые слова: категорирование; автоматизированные системы управления; безопасность; объекты КИИ; экологическая значимость.

METHODOLOGY FOR ASSESSING THE ENVIRONMENTAL SIGNIFICANCE OF THREATS TO A CII OBJECT ON THE EXAMPLE OF AN AUTOMATED PROCESS CONTROL SYSTEM OBJECT

Vladimir Derevyanko, *St. Petersburg state university of telecommunications n/a prof. M. A. Bonch-Bruevich.*

Annotation. In the modern world, attacks on automated control systems, including critical information infrastructure objects, are becoming more frequent. Successful malicious interventions can lead to negative consequences. In order to avoid this, it is necessary to strictly comply with the requirements and rules for categorizing CII objects, as well as to ensure the safety of the operation of control systems, including environmental ones.

Keywords: categorization; automated control systems; security; CII objects; ecological significance.

Введение

Вопрос категорирования является важным аспектом, которому необходимо уделять больше внимания. Необходимо соблюдать все требования и правила, согласно установленным постановлениям и приказам. При нарушении (не соблюдении) данных требований предприятие может нанести вред не только себе, но и окружающему миру.

В настоящее время в соответствии с постановлением Правительства РФ от 13 апреля 2019 г. № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127» все объекты критической информационной инфраструктуры (КИИ) подлежат обязательному категорированию. Существуют определенные правила и требования категорирования, а также показатели критериев значимости объектов КИИ и их значения. В постановлении Правительства Российской Федерации указаны следующие показатели значимости: социальная, политическая, экономическая, экологическая и значимость для обеспечения обороны страны, безопасности

государства и правопорядка. В данной статье будет рассмотрена экологическая значимость[1].

Исходя из Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», объектом КИИ являются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления (АСУ ТП) субъектов критической информационной инфраструктуры. В качестве объекта КИИ оценивалась автоматизированная система управления по переработке и утилизации отходов[2,3].

Показатель экологической значимости представляет собой вредные воздействия на окружающую среду, такие как ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия, оцениваемые следующими факторами:

а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям:

- вся территория одного муниципального образования или одной внутригородской территории города федерального значения;
- выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения;
- выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения.

б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек):

- более или равно 50, но менее 1000;
- более или равно 1000, но менее 5000;
- более или равно 5000.

В настоящее время существует множество видов угроз для АСУ ТП. Большинство из них направлено на вывод системы из строя. Успешное проведение атаки на систему может привести к негативным последствиям. Кроме того, вывод системы из строя может произойти, если не были соблюдены определенные правила и требования производства. В данном случае будет рассмотрен ущерб экологии на фоне информационных угроз, актуальных для АСУ по переработке и утилизации отходов.

---

[1] Постановление Правительства РФ от 8 февраля 2018 г. № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (дата обращения - май 2020).

[2]Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (дата обращения - май 2020).

[3] Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (дата обращения - май 2020).

Для обеспечения безопасности объектов критической информационной инфраструктуры необходимо проводить тщательный анализ угроз. В соответствии с подпунктом 1 пункта 11 приказа № 239 Федеральной службы по техническому экспорту и контролю, целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями, а также особенностей функционирования значимого объекта[4].

Анализ угроз безопасности информации должен включать:

- выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;
- анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;
- определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;
- оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

По результатам анализа угроз безопасности информации могут быть разработаны рекомендации по корректировке архитектуры значимого объекта и организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Рисунок 1

[4] Федеральный закон от 21.07.2011 N 256-ФЗ (ред. от 24.04.2020) «О безопасности объектов топливно-энергетического комплекса» (дата обращения - май 2020).

При успешной атаке на данную автоматизированную систему и вывод ее из строя, либо не соблюдении правил эксплуатации, нарушается или полностью останавливается производство по переработке, что может нанести большой ущерб экологии, а соответственно и населению. Отказ системы может привести к загрязнению воздуха, водоемов, скоплению мусора и т. д. Все это негативно окажет влияние не только на здоровье человека, но и на природные ресурсы. Помимо этого, последствия прекращения производства могут затронуть различного рода продукты и сельское хозяйство. Загрязнение воздуха и водоемов приведут за собой ухудшение качества продуктов, а при остановке производства на многочисленных и больших объектах, высока вероятность появления дефицита (рис. 1).

Ниже представлена классификация отходов по классам опасности и соответствующей степени воздействия на окружающую среду (табл. 1) [7].

Таблица 1.

Класс опасности	Степень негативного воздействия на окружающую среду	Негативные последствия для окружающей среды
1	очень высокая	**необратимое** нарушение экосистемы и **невозможность** восстановления экосистемы; крайне высокая степень негативного воздействия на организм человека.
2	высокая	**крайне высокая степень** нарушения экосистемы; ериод восстановления экосистемы от 30 лет с момента устранения источника негативного воздействия на экосистему и обезвреживания территории нахождения отходов данного класса опасности; крайне высокая степень негативного воздействия на организм человека.
3	умеренная	**умеренная степень опасности** для экосистемы; ериод восстановления экосистемы от 10 лет с момента устранения источника негативного воздействия на экосистему и обезвреживания территории нахождения отходов данного класса опасности; высокая степень негативного воздействия на организм человека.
4	низкая	**незначительная степень нарушения** экосистемы; период восстановления экосистемы от 3 лет с момента уничтожения источника негативного воздействия; меренная степень негативного воздействия на человека епосредственно в области нахождения отходов данного класса.
5	очень низкая	**нарушения экосистемы отсутствуют**, влияние на гомеостаз экосистемы отсутствует; не требуется очистка и восстановление экосистемы; негативное воздействие на человеческий организм отсутствует или отмечается в пределах допустимых (минимальных) показателей окружающей среды.

В соответствии с подпунктом е) пункта 10 постановления Правительства РФ от 8 февраля 2018 г. N 12 «Об утверждении Правил категорирования объектов

критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений», исходными данными для категорирования, в том числе, являются угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

Одним из инцидентов, повлекших за собой нанесение вреда экологии, является авария 18 апреля 2005 г. на заводе по переработке отходов и ядерного топлива «*THORP*» в Великобритании, в городе Селлафилд (рис. 2) [6].

Рисунок 2

Была обнаружена утечка высокорадиоактивных веществ. Авария произошла из-за повреждения трубы, соединявшейся с одним из резервуаров. Руководство предприятия признало, что были неисправны датчики, предупреждающие об утечке, в связи с чем персонал не смог вовремя среагировать на происшествие. В соответствии с 239 Приказом ФСТЭК при соблюдении требований проектирования системы оповещения и внедрения организационных и технических мер по обеспечению безопасности значимого объекта, можно было избежать негативных последствий. Требования к обеспечению безопасности включаются в техническое задание на создание значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, которые должны содержать:

- цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;
- категорию значимости значимого объекта;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;
- перечень типов объектов защиты значимого объекта;

- требования к организационным и техническим мерам, применяемым для обеспечения безопасности значимого объекта;
- стадии (этапы работ) создания подсистемы безопасности значимого объекта;
- требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;
- требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);
- требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями,
- требования к составу и содержанию документации, разрабатываемой в ходе создания значимого объекта.

После аварии ужесточился контроль поступающих в продажу продуктов питания, а из находящихся поблизости ферм продажа молочных продуктов была запрещена в течение шести недель.

Последствия аварии изучались Национальной комиссией по радиологической защите. По сделанной комиссией оценке, среди населения могло произойти около 30 дополнительных смертей от заболевания раком, то есть за время, в течение которого могут произойти эти 30 смертей, среди подвергшихся облучению людей вероятно умерло бы около 1 млн человек. В соответствии с правилами категорирования данный объект имел бы 2-ю категорию значимости [6].

При оценке экологического фактора в случае возникновения аварийной ситуации, помимо немедленного устранения проблем, следует проанализировать возможные последствия, к чему может привести затруднение или невозможность ликвидации угрозы и принять определенные меры. На примере вышеупомянутого инцидента на заводе «*THORP*», чтобы не допустить подобных ситуаций, необходимо регулярно проводить тестирование работоспособности всех систем, анализ безопасности систем, инструктаж персонала по технике безопасности, по поведению в экстренных ситуациях. В данном случае нужно было обратить особое внимание на правила и требования к эксплуатации оборудования [3].

Во время анализа последствий необходимо рассматривать все возможные сценарии ущерба: на какую территорию может распространиться загрязнение воздуха (водоемов), сколько людей могут пострадать, каков будет урон природному и животному миру, а также за какие сроки можно устранить неполадки. При оценке ущерба следует опираться на показатели экологической значимости, т. е. насколько велика территория и количество населения, которые могут быть подвержены вредным воздействиям, чтобы оценить масштабы угрозы. Для того, чтобы избежать или минимизировать подобные ситуации, необходимо соблюдать определенные требования и правила.

Недооценка угроз безопасности информации может повлечь множество негативных, а нередко и разрушительных последствий. Примером таких последствий является атака на немецкий промышленный завод *THYSSEN KRUPP*. Злоумышленники проникли в компьютер, управляющий доменной печью, установили вредоносную программу, которая заставили печь перегреться и расплавиться, что повлекло за собой существенный вред всей системе. В данном случае проблема была с защитой от удаленного взлома системы. Для повышения взломостойкости следует регулярно обновлять базы сигнатур, устанавливать надежные файрволы и проводить диагностику оборудования [5].

Другим примером является случай на заводе *MAROOCHY WATER SERVICES* в Австралии. Уволенный из компании инженер получил несанкционированный удаленный доступ через направленную антенну и три месяца сливал неочищенные сточные воды, управляя помпами, в результате чего миллионы литров сточных вод попали в ближайшую реку, что привело также к затоплению местной гостиницы. Случай схож с тем, что произошло на немецком заводе, рассмотренном выше. При соблюдении всех требований, регулярном тестировании систем на предмет удаленного вмешательства, последствия могли быть иными. Инцидент повлек за собой существенные экологические проблемы и расходы компании на предотвращение катастрофы. Данный пример наглядно демонстрирует, что даже из-за одного человека могут произойти масштабные экологические проблемы, которые, в свою очередь, могут нанести вред населению [4].

Анализируя наиболее известные инциденты, связанные с экологическим ущербом, можно сделать выводы, что при обеспечении безопасности объектов критической информационной инфраструктуры функционирующих для переработки и утилизации отходов, необходимо обратить внимание на выполнение требований, предъявляемых к подсистемам безопасности и на злоумышленников, использующих против информационных систем такие уязвимости, как удаленное выполнение кода, переполнение кода, внедрение вирусных программ, отказ в обслуживании и т. д.

Заключение

Подводя итог, можно утверждать, что изначальный своевременный и качественный подход к категорированию объекта позволил бы внедрить требования по обеспечению безопасности и избежать негативных последствий не только в экологической, но других сферах жизнедеятельности.

Литература

1. АСУ ТП https://studwood.ru/2155750/tehnika (дата обращения - май 2020).
2. Атаки на кибербезопасность https://www.mitre.org/publications/technical-papers/malicious-control-system/ (дата обращения - июнь 2020).
3. Защита информации http://www.ltddash.by/acy-тп-защита-информации (дата обращения - июнь 2020).
4. Информационная безопасность АСУ ТП https://habr.com/ru/post/316184/ (дата обращения - июнь 2020).
5. Угрозы информационной безопасности https://www.anti-malware.ru/threats/information-security-threats (дата обращения - июнь 2020).
6. THORP https://bellona.ru/2005/06/08/ (дата обращения - июнь 2020).
7. Waste https://www.recomo.ru/ (дата обращения - июнь 2020).