Доверие и безопасность в информационном обществе

СТРАХОВАНИЕ КИБЕР-РИСКОВ АЭС – ВОПРОСЫ СОГЛАСОВАНИЯ УСЛОВИЙ И ПОДХОДОВ К ОЦЕНКЕ РИСКОВ

Статья рекомендована к публикации членом редакционного совета А.Н. Райковым 18.03.2023

Саченко Лариса Анатольевна

Кандидат экономических наук
ООО «Риск-профиль», генеральный директор
Москва, Российская Федерация
sachenko@risk-profile.ru

Деревянкин Александр Альбертович

Кандидат технических наук
Московский государственный технический университет имени Н. Э. Баумана, доцент
Москва, Российская Федерация
aderevyankin@outlook.com

Берберова Мария Александровна

Кандидат технических наук
МИРЭА – Российский технологический университет, Институт искусственного интеллекта, Кафедра промышленной информатики, доцент
Москва, Российская Федерация
maria.berberova@gmail.com

Деревянкин Глеб Александрович

Московский государственный технический университет имени Н. Э. Баумана, инженер, аспирант
Москва, Российская Федерация
work333@mail.ru

Аннотация

Рост масштабов использования цифровых технологий в современных атомных электростанциях (АЭС) приводит к развитию нового класса угроз с кибер-источниками рисков. При этом возникает проблема формирования адекватной финансовой защиты атомных станций на случай реализации таких событий. Цель настоящей статьи – разработка алгоритма по использованию имеющихся отраслевых методов и данных по оценке рисков для организации эффективной страховой защиты АЭС от кибер-рисков. Для этого выполнен совместный анализ существующих страховых продуктов по страхованию кибер-рисков и структуры кибер-рисков АЭС, а также предложен подход по разработке качественных и количественных условий страхования рисков АЭС, включающий рассмотрение кибер-рисков, на основе использования сюрвейерских оценок. Те же методы могут быть использованы впоследствии для разработки программ страхования кибер-рисков для промышленных и энергетических предприятий.

Ключевые слова

страхование кибер-рисков, атомные электростанции, анализ рисков, предстраховая экспертиза

Введение

Организация страховой защиты атомных электростанций от кибер-рисков представляет собой задачу повышенной актуальности и повышенной сложности. Страховой рынок, после нескольких лет поступательного развития страхования кибер-рисков, столкнулся с рядом серьезных убытков.

https://doi.org/10.52605/16059921_2024_02_112

Вследствие этого подвергаются пересмотру в сторону сокращения как состав рисков, так и размеры страховых сумм. Очевидно, что страховщики нуждаются в более углубленном анализе риска для дальнейшего развития кибер-страхования. С точки зрения малых и средних предприятий требуется получение статистических данных. Однако для крупных промышленных предприятий и особенно для предприятий атомной отрасли, такой подход невозможен в силу крайне низкой вероятности страховых событий. В то же время, именно низкие вероятности и серьезный размер потенциальных убытков привели к развитию исследований по вероятностному анализу безопасности (ВАБ) атомных станций и методам предстраховой экспертизы атомных объектов. Результаты этих исследований уже несколько десятков лет успешно применяются при страховании гражданской ответственности за ядерный ущерб и страховании имущества атомных станций.

Цель настоящей статьи – разработка алгоритма по использованию имеющихся отраслевых методов и данных по оценке рисков для организации эффективной страховой защиты АЭС от кибер-рисков.

Для этого во втором разделе проанализированы существующие на текущий момент методические подходы к решению проблем изменчивости и неоднородности кибер-рисков, выделены подходы, наиболее актуальные с точки зрения характерных рисков для атомных станций.

Во третьем разделе проведен качественный анализ существующих страховых продуктов по кибер-страхованию, выделены условия, наиболее соответствующие потребностям АЭС как страхователей. Также проведено выделение имеющихся «пробелов» в описании рисков, ограничивающих применение кибер-страхования для атомных предприятий.

Четвертый раздел посвящен методам выделения наиболее значимых рисков АЭС вследствие использования цифровых технологий. Основные предлагаемые для этого методы – применение методов предстраховой экспертизы с включением кибер-источников рисков.

1 Подходы и проблемы при оценке условий страхования кибер-рисков

К настоящему моменту накоплено достаточное количество теоретических подходов и некоторое количество статистических данных по результатам функционирования рынка кибер-страхования. Основная трудность при оценке условий страхования кибер-рисков, выделяемая многими исследователями, например, [1-3], заключается в изменчивости характера воздействия кибер-угроз. Если в традиционных видах страхования моделирование страховщиками будущих исков основано на анализе исторических данных, то для области кибер-страхования это невозможно, поскольку типы и направленность кибер-угроз постоянно модифицируются.

Вследствие этого возникают сложности в определении причинно-следственных связей между источником риска и характером последствий. Применение сценарных методов [1,4] и оценка отдельных угроз [5] несколько снижают степень неопределенности относительно процесса развития события от факторов риска до ущерба, но, как правило, не могут быть основаны на количественных оценках риска в силу отсутствия статистических данных.

Высокая скорость изменения угроз затрудняет, также, формирование унифицированной терминологии относительно договоров кибер-страхования. Европейское агентство кибербезопасности ENISA провело исследование [6], которое выявило совершенно различные определения и подходы к оценке одних и тех же рисков у крупнейших европейских страховщиков.

Помимо терминологической незрелости, рынок кибер-страхования столкнулся с тем, что страховые случаи по данному виду не соответствуют необходимым критериям пригодности риска к страхованию. Так, значимыми критериями для признания риска страховым являются: случайный характер событий, возможность проведения идентификации и оценки риска, ограничение катастрофических потерь, значительное количество независимых субъектов с однородным набором рисков, умеренный размер средних ожидаемых убытков [7]. Статистическое исследование [8], выполненное на базе крупнейшей базы данных США по кибер-убыткам Advisen[1], выявило сложную и неоднородную природу кибер-рисков. С одной стороны, исследование статистически подтверждает различия по характеру и вероятности убытка, а также тяжести последствий по отраслям, типам и размеру компаний. С другой стороны, показано, что распределения убытков характеризуются тяжелыми «хвостами», а определяющую роль в финансовом результате будут играть не средние значения, а наличие или отсутствие одного экстремального события вне

[1] https://www.advisenltd.com/

зависимости от типа риска и отрасли. Еще одним существенным препятствием для причисления кибер-рисков к разряду страховых является выявленная кумуляция[2] и взаимосвязь между такими рисками [9].

Несмотря на довольно серьезные методологические препятствия, необходимость организации страховой защиты от кибер-рисков приводит к развитию новых для страховой отрасли подходов к оценке рисков: от качественных и полуколичественных до количественных. Одним из наиболее распространенных является метод FAIR[3] [10], который основан на классифицированной системе факторов риска и качественно-количественных оценках. К главным преимуществам метода можно отнести универсальность относительно области применения и системный подход, что позволяет сформировать общее представление, выделить приоритетные угрозы и провести приближенную оценку возможных убытков. Однако высокая степень обобщения, а также отсутствие рассмотрения конкретных событий и временных характеристик существенно ограничивают область применимости результатов, полученных при помощи данного метода. К модификациям подобного метода, учитывающим временные характеристики кибер-угроз, можно отнести подход [1]. Применение метода Монте-Карло предлагается в методике [11] для получения распределения убытков и оценки «кибер-стоимости под риском», по аналогии с методикой «стоимость под риском». Данный метод предполагает более количественно-определенный результат оценки риска по сравнению с вышеописанными методами, однако при этом также существует довольно высокая степень обобщения. Кроме того, требуется достаточное количество статистических данных по реализации отдельных угроз для получения исходных распределений. При недостаточности данных результат будет во многом зависеть от субъективных оценок. Для случаев, когда размер ущерба страхователя подчиняется экспоненциальному распределению, в работе [12] проведено моделирование ожидаемого ущерба страховщика для разных вариантов страхования, предложены схемы корректировки тарифа по системе бонус-малус при осуществлении страхователем превентивных мероприятий. Как и в случаях выше, основное ограничение данного метода – опора на стабильные средние значения, в то время как природа кибер-рисков экстремальная и изменчивая.

Направление по применению методов искусственного интеллекта в кибер-страховании теоретически довольно перспективно, но пока недостаточно разработано. На текущий момент можно упомянуть работу [13], в которой выполнен анализ факторов, влияющих на величину убытков при реализации кибер-рисков. Для этого авторы предложили сочетание рангового метода оценки параметров регрессионной модели и подход декомпозиции Шепли-Лоренца. Результаты расчетов выражены обобщенным рейтинговым показателем, они выявляют факторы риска, наиболее приоритетные с точки зрения страхования и других управляющих мер, но не оценивают размер возможных финансовых потерь.

Наиболее близкими к задачам кибер-страхования атомных предприятий являются методы анализа видов и последствий отказов[4]. Например, в статье [14] метод применяется для приоритизации кибер-рисков для объектов критической инфраструктуры. Также с точки зрения актуальности для атомных станций следует рассмотреть модели, рассматривающие конкретные сценарии развития событий в кибер-физических системах [15-17]. Авторы [15] используют оценки вероятности исходных событий и возможных эффектов для выбора оптимальных мер реагирования на случившиеся события.

Суммируя вышеизложенное, можно сделать вывод о том, что к настоящему моменту не сформирован универсальный методологический подход к оценке потенциальных воздействий кибер-угроз и оценке условий страхования. Тем не менее, использование методов, соответствующих конкретным частным задачам, может быть весьма продуктивным и послужить основой для расширенного применения в дальнейшем.

---

[2] Совокупность страховых рисков, при которых большое количество объектов страхования со значительными страховыми суммами могут быть затронуты одним и тем же страховым случаем (например, землетрясением). Выступает как сосредоточение рисков в пределах ограниченного пространства в единицу времени (Ефимов С.Л. Экономика и страхование: Энциклопедический словарь. – М.: Церих-ПЭЛ, 1996. – 528 с. – ISBN 5-87811-016-4.).

[3] FAIR (Factor Analysis of Information Risk), Факторный анализ информационного риска

[4] Failure Mode and Effect Analysis (FMEA)

2 Типы полисов и страховых покрытий, наиболее актуальные для АЭС

Согласно стандарту ИСО 27102:2019[5], для кибер-страхования рекомендованы следующие определения:

- кибер-инцидент - кибер-событие, которое влечет за собой потерю информационной безопасности или влияет на бизнес-процессы;
- кибер-риск – риск, вызванный кибер-угрозой;
- кибер-угроза – угроза в связи с использованием киберпространства;
- киберпространство - взаимосвязанная цифровая среда сетей, сервисов, систем и процессов.

Таким образом, при идентификации кибер-рисков в целях страхования, принципиальным моментом является принадлежность источника риска к киберпространству. При этом ущерб может распространяться за пределы киберпространства и нарушать основные процессы. Такой риск характерен для кибер-физических систем. Например, один из наиболее известных случаев такого рода в атомной отрасли произошел в 2010 году, когда вирус Stuxnet поразил более 1000 из 5000 центрифуг на иранском заводе по обогащению урана[6] и привел к приостановке работы АЭС в Бушере.

По типу покрытия полисы кибер-страхования бывают самостоятельными либо могут входить в состав имеющихся договоров страхования имущества и гражданской ответственности.

В российской практике самостоятельные полисы кибер-страхования относятся к страхованию операторов данных. Изначально данный вид страхования разрабатывался для США и, затем, для европейских стран в связи с принятием законодательства о защите персональных данных. Такое страхование преимущественно направлено на возмещение расходов и ответственности, связанных с нарушением персональных данных или корпоративной информации, а также цифровых активов. Поскольку деятельность атомных станций не направлена на обработку больших объемов персональных данных, актуальность приобретения такого полиса для них невысока. Тем не менее, эти же правила страхования операторов данных позволяют застраховать убытки при нарушении или прекращении функционирования компьютерной системы в части недополученной прибыли. Такую возможность теоретически можно использовать для страхования недополученной прибыли вследствие перерывов в производстве, вызванных кибер-инцидентами. Но для практического применения на страховом рынке такая задача выглядит труднореализуемой, поскольку возникает масса специфических вопросов по функционированию автоматизированных систем управления АЭС, которые должны быть отражены в условиях договоров и правил страхования. Помимо этого, данный вид страхования относится к страхованию финансовых рисков, что не является оптимальным с точки зрения налогообложения.

Второй вариант, который представляется более целесообразным с точки зрения потребностей атомных станций и реализуемым на практике - внедрение условий страхования кибер-рисков в действующие договоры страхования имущества и гражданской ответственности АЭС.

Действительно, с точки зрения возможных последствий, наиболее значимыми рисками АЭС являются радиационные аварии. Вследствие таких событий возможно возникновение гражданской ответственности за ядерный ущерб в серьезном масштабе. Например, в результате аварии на АЭС Фукусима суд постановил взыскать[7] с руководителей компании-владельца Tokyo Electric Power Company (Tepco) сумму 13 триллионов иен (или около 95 млрд. долл.). При курсе доллара к рублю на уровне 76 это составит примерно 7,2 трлн. руб. В соответствии с условиями Венской Конвенции по ответственности за ядерный ущерб в редакции 1963 года оператор российских АЭС АО «Концерн Росэнергоатом» обязан поддерживать страхование или другую форму финансового обеспечения на сумму не менее, чем 5 миллионов долларов США по золотому паритету на 29 апреля 1963 года за каждый ядерный инцидент[8]. В ценах 2022 года это составляет 20, 6 млрд. руб., и в таком объеме в настоящее время осуществляется страхование гражданской ответственности за ядерный ущерб в АО «Концерн Росэнергоатом». Договор страхования заключен на условиях «от всех рисков», при этом логично предположить, что и от последствий кибер-инцидентов тоже. Тем не менее, в последние годы на страховом рынке сложилась тенденция по скрытому исключению последствий кибер-рисков из состава такого типа покрытия, если иное не специально не

[5] ISO/IEC 27102:2019, Information security management—Guidelines for cyber-insurance (2019)
[6] https://www.kaspersky.ru/about/press-releases/2014_stuxnet-v-detaliakh
[7] https://edition.cnn.com/2022/07/13/business/tokyo-court-fukushima/index.html
[8] Венская Конвенция о гражданской ответственности за ядерный ущерб (Вена, 21 мая 1963 г.).

оговаривается в договоре страхования. С точки зрения страховой компании, добавление нового класса причин катастрофического события приводит к изменению степени риска, следовательно, является причиной для пересмотра условий страхования. С точки зрения Страхователя, автоматизированные системы управления технологическими процессами АЭС использовались на протяжении предыдущих периодов страхования, и степень риска одномоментно не изменилась. Поэтому проведение оценки риска наступления гражданской ответственности за ядерный ущерб вследствие кибер-инцидента поможет прояснить и согласовать позиции сторон по данному вопросу в случае разногласий.

Второй по значимости вид ущерба от радиационных аварий – ущерб имуществу. В предельном случае он может доходить и даже превышать стоимость сооружения АЭС, которая приблизительно равна 280 млрд. руб.[9] Здесь ситуация со страхованием совершенно другая, чем в случае страхования гражданской ответственности. Чаще такие договоры заключаются на условиях «от поименованных рисков». В таком случае, основные виды кибер-инцидентов, как причины имущественного ущерба, должны быть включены как в текст договора страхования, так и в текст правил страхования. Например, по договорам страхования от поломок оборудования, в состав покрытия включаются, в частности, такие причины событий:

- ошибки / недостатки конструирования, проектирования расчетов;
- ошибки / недостатки изготовления, монтажа, наладки и ремонта;
- непреднамеренные ошибки / неправильные действия персонала Страхователя при использовании и обслуживании застрахованного имущества и т.п.

Аналогичные формулировки необходимо выработать и для кибер-инцидентов. Исходя из такой постановки задачи, уже нельзя ограничиться оценкой совокупного увеличения ожидаемого ущерба, как в случае страхования «от всех рисков», и возникает необходимость покомпонентной оценки рисков. Учитывая наличие упомянутых в предыдущем разделе терминологических затруднений, для формирования полноценного страхового продукта необходимо:

- согласовать точные формулировки наиболее значимых видов кибер-инцидентов, приводящих к имущественному ущербу АЭС;
- провести количественную оценку риска по выделенным группам событий.

Третий по значимости вид ущерба вследствие аварий на АЭС - недополученная прибыль вследствие прекращения работы блока или длительного перерыва в работе блока. Приблизительную оценку возможных потерь при полной потере одного блока можно выполнить следующим способом. На момент 2022 года средняя мощность блока составляет 796 МВт, средний предполагаемый остаточный срок эксплуатации – 20 лет. Тогда при ставке дисконтирования 15 % и примерной оптовой стоимости электроэнергии для производителей 1470 руб./МВт-ч., примерная стоимость недовыработки среднего гипотетического потерянного блока составит около 58 млрд. руб. С точки зрения практики страхования, случаи недополучения прибыли вследствие перерывов в производстве, вызванных ущербом имуществу, могут быть отнесены к страхованию имущества. Следовательно, обозначенный в предыдущем абзаце объем работ по согласованию формулировок наиболее значимых рисков и проведению оценки этих рисков позволит охватить страховой защитой не только события с прямым ущербом имуществу по причине кибер-инцидентов, но и события, сопровождающиеся недополучением прибыли вследствие перерывов в производстве электроэнергии по этим же причинам.

Таким образом, исходя из структуры наиболее значимых рисков АЭС, предпочтительным выглядит вариант по включению условий страхования кибер-рисков в действующие договоры страхования, что предполагает проведение работ по качественной и количественной оценке кибер-рисков и согласованию приемлемых условий на страховом рынке.

3 Подходы к оценке кибер-рисков с помощью предстраховой экспертизы

С точки зрения подхода к оценке кибер-рисков АЭС, основным итогом рассмотрения материала предыдущих разделов являются два момента:

- в области кибер-страхования на настоящий момент не сформирована универсальная методология по оценке риска;

[9] gaz.ru/news/nuclear/743181-rosatom-planiruet-nachat-stroitelstvo-vtoroy-ocheredi-leningradskoy-aes-2-v-2024-godu/

- предпочтительным вариантом страхового покрытия АЭС является интеграция кибер-рисков в действующие программы страхования имущества и гражданской ответственности.

Руководствуясь этими исходными положениями, логично воспользоваться действующими методиками по оценке рисков гражданской ответственности и ущерба имуществу АЭС с включением кибер-рисков, наряду с уже включенными в рассмотрение типами инициирующих событий.

Согласно сегодняшней практике страхования, при проведении сюрвейерских оценок рисков АЭС в общем случае используется следующий алгоритм (рисунок 1):

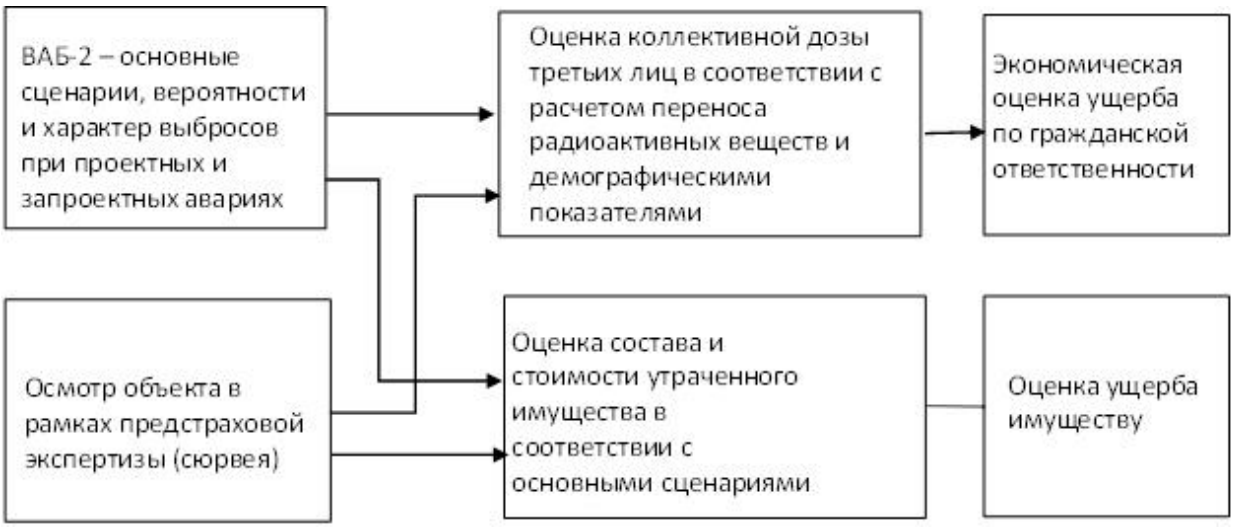

Рисунок 1: *Общая схема процесса проведения оценки страховых рисков АЭС.*

Для корректного включения кибер-рисков в качестве инициирующих событий в представленный на рисунке 1 алгоритм, необходимо понимать, что автоматизированные системы управления технологическими процессами (АСУ ТП) АЭС обладают массой отличий от большинства информационных систем.

Во-первых, если в большинстве корпоративных информационных систем критическим цифровым активом является информация, то для АСУ ТП АЭС - это сам технологический процесс, его непрерывность, целостность и безопасность.

Во-вторых, сложность структуры АСУ ТП АЭС, которая содержит сотни тысяч источников сигналов, оказывающих влияние на объект управления. Из этих сигналов десятки тысяч привязаны к физическому оборудованию. Отдельные подсистемы объединены в единую централизованную систему управления верхним уровнем АСУ ТП.

В-третьих, необходимость рассмотрения полного цикла этапов жизненного цикла АСУ ТП АЭС для корректной оценки рисков: от проектирования, разработки и системной интеграции до вывода из эксплуатации. Такая необходимость обусловлена влиянием уязвимости АСУ ТП вне этапа эксплуатации на проявление рисков во время этапа эксплуатации.

При проведении предстраховой оценки рисков АЭС, включающей блок кибер-рисков, основными объектами для анализа могут быть модель нарушителя, модель угроз, анализ защищенности объекта, оценка готовности к реагированию.

В руководстве МАГАТЭ по компьютерной защищенности для ядерной защищенности[10] указывается, что при разработке модели угроз отдельные угрозы могут быть классифицированы разными способами. В данном руководстве рассматриваются преимущественно преднамеренные противоправные угрозы и дано следующее определение: «угроза - это лицо или группа лиц, обладающих мотивацией, намерением и способностью совершить злонамеренное деяние. Любое лицо, совершающее или пытающееся совершить злонамеренное действие, является противником».

[10] IAEA Nuclear Security Series No. 42-G. Computer Security for Nuclear Security. Implementing Guide. IAEA, Vienna, 2021.

В то же время, в техническом руководстве МАГАТЭ по компьютерной безопасности[11] особое внимание уделено инсайдерам в силу имеющихся у них прав доступа к компьютерным системам. При их классификации не все категории инсайдеров отнесены к злоумышленникам, и выделены следующие категории: пассивный инсайдер, активный инсайдер и невольный инсайдер. Возможны, также, непреднамеренные ошибки персонала.

Помимо значительного влияния человеческого фактора, остается возможность технологических отказов аппаратного и программного обеспечения.

В исследовании, посвященном анализу типов и размеров убытков по различным отраслям [18], наиболее значимыми событиями для промышленных предприятий, сопровождающимися серьезными размерами убытков, выделено воздействие вредоносного кода и атаки типа «отказ в обслуживании».

В качестве основных аспектов защищенности объекта рассматривают[12] множество факторов, из которых выделены основные:

- общее управление организацией;
- технологические аспекты;
- человеческий фактор;
- текущее и сервисное обслуживание;
- внешнее и внутреннее окружение.

Совместное рассмотрение модели угроз, аспектов защищенности и готовности к реагированию может быть исходным материалом для выполнения экспертной или количественной оценки возможных сценариев с выходом на физическое оборудование. Для целей страхования не требуется высокая сценарная детализация и приоритизация, поэтому полученные оценки далее можно использовать для коррекции уже имеющихся сюрвейерских результатов по следующему алгоритму (рисунок 2):

Рисунок 2: *Логика включения кибер-рисков в оценку страховых рисков АЭС*

Поскольку при проведении классического сюрвея оценка размеров возможного ущерба уже выполнена, изменение степени риска за счет включения группы кибер-рисков произойдет за счет роста вероятности страхового случая. При этом, коррекция вероятности страхового случая при реализации кибер-риска может быть оценена по формуле Байеса:

$$P(\text{Ущерб}|\text{Кибер}) = P(\text{Ущерб})\frac{P(\text{Кибер}|\text{Ущерб})}{P\ (\text{Кибер})},$$

где:

$P(\text{Ущерб}|\text{Кибер})$ - вероятность наступления ущерба при реализации кибер-риска;

$P(\text{Ущерб})$ - оценка вероятности наступления ущерба в результате классического сюрвея (предстраховой экспертизы);

$P(\text{Кибер}|\text{Ущерб})$ – оценка вероятности реализации кибер-риска при наступлении ущерба;

$P\ (\text{Кибер})$ – оценка вероятности реализации киберриска.

Для верификации части полученных результатов возможно использование статистики отказов систем контроля, тепловой автоматики и измерений.

При таком подходе включенные количественные оценки будут иметь точное описание категории инициирующих событий. Это позволит совместить для страховых целей качественные формулировки и соответствующие им количественные оценки для включения их в условия договора страхования.

[11] IAEA Nuclear Security Series No. 17-T (Rev. 1). Computer Security Techniques for Nuclear Facilities. Technical Guidance. IAEA, Vienna, 2021.
[12] https://os.kaspersky.ru/media/Kaspersky-Lab-cybersecurity-for-SCADA-ICS-Ru.pdf

Выводы

В статье на основе анализа современных методов оценки рисков в кибер-страховании и выделения предпочтительных вариантов структуры страховой защиты от кибер-рисков для атомных станций предложен подход по согласованию формулировок условий страхования и проведения количественной оценки рисков с включением класса кибер-рисков. Подход основан на использовании имеющихся результатов сюрвейерских оценок, скорректированных за счет включения инициирующих событий, относящихся к кибер-рискам.

Для практической реализации предложенного подхода необходимо провести обучение специалистов по кибербезопасности АЭС на предмет условий договоров страхования и методологии проведения сюрвейерских оценок. Таким образом, в связи с ростом масштабов использования цифровых технологий в современных АЭС, возникает необходимость расширения деятельности в области предстраховой экспертизы на область кибер-рисков.

Благодарности

Материал был представлен на 11-й Международной конференции «Физико-техническая информатика (СРТ2023)», 16-19 мая 2023 г., Пущино, Московская область, Россия.

Литература

1. Pavlík, L., Ficek M., Rak J. Dynamic Assessment of Cyber Threats in the Field of Insurance // Risks 10: 222. 2022. https://doi.org/10.3390/risks10120222
2. Mirsanova, O. On the Way to a Stable World: Security and Sustainable Development. // Analysis and sistematisation of basic pricing models and approaches in cyber risk insurance. San Diego, CA. 2015. DOI: 10.17809/02(2015) -04
3. Tsohou, A., Diamantopoulou, V., Gritzalis, S., Lambrinoudakis, C. Cyber insurance: state of the art, trends and future directions // International Journal of Information Security. 2023. Vol. https://doi.org/10.1007/s10207-023-00660-8
4. Rios Insua, D., Couce-Vieira, A., Rubio, J., Pieters, W., Labunets, K., Rasines, D. An Adversarial Risk Analysis Framework for Cybersecurity 2019. arXiv:1903.07727v1 [cs.CR]
5. Борхаленко В. Механизмы страхования в управлении рисками информационной безопасности // Экономический анализ: теория и практика. 2017. Т. 16. http://www.fin-izdat.ru/journal/analiz/. pp. 379-388.
6. ENISA. Commonality of risk assessment language in cyber insurance —Recommendations on Cyber Insurance. 2017. URL: https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance
7. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A. "Cyber-insurance survey," // Comput. Sci. Rev., No. 24, 2017. pp. 35–61.
8. Malavasi, M., Peters, G., Shevchenko, P., Truck, S., Jang, J., Sofronov, G. "Cyber Risk Frequency, Severity and Insurance Viability," No. arXiv:2111.03366v1 [, 2021.
9. Baer, W., Parkinson, A. "Cyberinsurance in it security management," // IEEE Secur. Priv, Vol. 5, 2007. pp. 50-56.
10. Freund, J., Jones, J. "Measuring and Managing Information Risk. A FAIR Approach.," Butterworth-Heinemann is an imprint of Elsevier, ISBN: 978-0-12-420231-3, 2015.
11. Erola, A., Agrafiotis I., Nurse J., Axon L., Goldsmith M., Creese S.A system to calculate Cyber Value-at-Risk // Computers & Security. 2022. Vol. 113. https://doi.org/10.1016/j.cose.2021.102545
12. Гераськин, М., Ростова, Е. "Влияние превентивных мер на условия страхования риска в кибер-физической системе промышленного предприятия" // Математические методы в технологиях и технике, Т. 5, DOI 10.52348/2712-8873_MMTT_2021_5_34, 2021. С. 34-37.
13. Giudici, P, Raffinetti E. Explainable AI methods in cyber risk management // Qual Reliab. 2021. https://doi.org/10.1002/qre.2939. pp. 1-9.
14. Oliveira, J., Carvalho G., Cabral B., Bernardino J. Failure Mode and Effect Analysis for Cyber-Physical Systems // Future Internet. Dec 2020. doi:10.3390/fi12110205. P. 205.
15. Singh, U., Sharma A.,Singh S., Upreti K. et al. Cyber Physical Systems: Concepts and Applications. CRC Press, 2023. DOI: 10.1201/9781003220664-9 pp.

16. Skytterholm, A., Hotvedt G. Criteria for Realistic and Expedient Scenarios for Tabletop Exercises on Cyber Attacks Against Industrial Control Systems in the Petroleum Industry // International Conference on Cybersecurity, Situational Awareness and Social Media. 2023. Vol. DOI: 10.1007/978-981-19-6414-5_3
17. Гаськова, Д., Массель, А. "Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры," // Вопросы кибербезопасности, Vol. 2(30), No. DOI: 10.21681/2311-3456-2019-2-42-49, 2019. pp. 42-49.
18. Shevchenko, P., Jang J.,Malavasi M., Peters G, Sofronov G., Trück S. "The nature of losses from cyber-related events: risk categories and business sectors," // Journal of Cybersecurity, 1-12 2022. https://doi.org/10.1093/cybsec/tyac016

NPP CYBER RISK INSURANCE – ISSUES OF WORDINGS AND APPROACHES TO RISK ASSESSMENT COORDINATION

Sachenko, Larisa Anatolievna

Candidate of economic sciences
Risk-profile LLC, CEO
Moscow, Russian Federation
sachenko@risk-profile.ru

Derevyankin, Aleksandr Albertovich

Candidate of technical sciences
Bauman Moscow State Technical University, associate professor
Moscow, Russian Federation
aderevyankin@outlook.com

Berberova, Maria Aleksandrovna

Candidate of technical sciences
MIREA – Russian Technological University, Institute of artificial intelligence, Department of industrial informatics, associate professor
Moscow, Russian Federation
maria.berberova@gmail.com

Derevyankin, Gleb Aleksandrovich

Bauman Moscow State Technical University, engineer, graduate student
Moscow, Russian Federation
work333@mail.ru

Abstract

The growing use of digital technologies in modern nuclear power plants (NPP) leads to the development of a new class of threats with cyber sources of risks. As a result of this process, a problem of forming adequate financial protection of nuclear power plants in case of such events arises. The purpose of this article is to develop an algorithm for using existing industry methods and risk assessment data to organize effective insurance protection of nuclear power plants from cyber risks. For this purpose, a joint analysis of existing insurance products for cyber risk insurance and the structure of nuclear power plant cyber risks was carried out. Based on the analysis, an approach to the development of qualitative and quantitative conditions for NPP risk insurance is proposed, including consideration of cyber risks based on the use of insurance survey assessments. The same methods can be used afterwards to develop cyber risk insurance programs for industrial and energy enterprises.

Keywords

cyber risk insurance, nuclear power plants, risk assessment, insurance survey

References

1. Pavlík, L., Ficek M., Rak J. Dynamic Assessment of Cyber Threats in the Field of Insurance // Risks 10: 222. 2022. https://doi.org/10.3390/risks10120222
2. Mirsanova, O. On the Way to a Stable World: Security and Sustainable Development. // Analysis and sistematisation of basic pricing models and approaches in cyber risk insurance. San Diego, CA. 2015. DOI: 10.17809/02(2015) -04
3. Tsohou, A., Diamantopoulou, V., Gritzalis, S., Lambrinoudakis, C. Cyber insurance: state of the art, trends and future directions // International Journal of Information Security. 2023. Vol. https://doi.org/10.1007/s10207-023-00660-8
4. Rios Insua, D., Couce-Vieira, A., Rubio, J., Pieters, W., Labunets, K., Rasines, D. An Adversarial Risk Analysis Framework for Cybersecurity 2019. arXiv:1903.07727v1 [cs.CR].
5. Borkhalenko V. Mekhanizmy strakhovania v upravlenii riskami informacionnoi bezopasnosti // Ekonomicheskii analiz: teoria i praktika. 2017. T. 16. http://www.fin-izdat.ru/journal/analiz/. pp. 379-388.

6. ENISA. Commonality of risk assessment language in cyber insurance —Recommendations on Cyber Insurance. 2017. URL: https://www.enisa.europa.eu/publications/commonality-of-risk-assessment-language-in-cyber-insurance
7. Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A. Cyber-insurance survey // Comput. Sci. Rev., No. 24, 2017. pp. 35–61.
8. Malavasi, M., Peters, G., Shevchenko, P., Truck, S., Jang, J., Sofronov, G. Cyber Risk Frequency, Severity and Insurance Viability. No. arXiv:2111.03366v1 [2021].
9. Baer, W., Parkinson, A. Cyberinsurance in it security management // IEEE Secur. Priv, Vol. 5, 2007. pp. 50-56.
10. Freund, J., Jones, J. Measuring and Managing Information Risk. A FAIR Approach. Butterworth-Heinemann is an imprint of Elsevier, ISBN: 978-0-12-420231-3, 2015.
11. Erola, A., Agrafiotis I., Nurse J., Axon L., Goldsmith M., Creese S.A system to calculate Cyber Value-at-Risk // Computers & Security. 2022. Vol. 113. https://doi.org/10.1016/j.cose.2021.102545
12. Geras'kin M., Rostova Ye. Vliyaniye preventivnykh mer na usloviya strakhovaniya riskov v kiberfizicheskoy sisteme promyshlennogo predpriyatiy // Matematicheskiye metody v tekhnologiyakh i tekhnike, T. 5, DOI 10.52348/2712-8873_MMTT_2021_5_34, 2021. S. 34-37.
13. Giudici, P, Raffinetti E. Explainable AI methods in cyber risk management // Qual Reliab. 2021. https://doi.org/10.1002/qre.2939. pp. 1-9.
14. Oliveira, J., Carvalho G., Cabral B., Bernardino J. Failure Mode and Effect Analysis for Cyber-Physical Systems // Future Internet. Dec 2020. doi:10.3390/fi12110205. P. 205.
15. Singh, U., Sharma A., Singh S., Upreti K. et al. Cyber Physical Systems: Concepts and Applications. CRC Press, 2023. DOI: 10.1201/9781003220664-9 pp.
16. Skytterholm, A., Hotvedt G. Criteria for Realistic and Expedient Scenarios for Tabletop Exercises on Cyber Attacks Against Industrial Control Systems in the Petroleum Industry // International Conference on Cybersecurity, Situational Awareness and Social Media. 2023. Vol. DOI: 10.1007/978-981-19-6414-5_3
17. Gas'kova, D., Massel', A. Tekhnologia analiza kiberugroz i ocenka riskov narushenia kiberbezopasnosti kriticheskoi infrastruktury // Voprosy kiberbezopasnosti, Vol. 2(30), No. DOI: 10.21681/2311-3456-2019-2-42-49, 2019. pp. 42-49.
18. Shevchenko, P., Jang J., Malavasi M., Peters G, Sofronov G., Trück S. The nature of losses from cyber-related events: risk categories and business sectors // Journal of Cybersecurity, 1-12 2022. https://doi.org/10.1093/cybsec/tyac016