Методы и системы защиты информации, информационная безопасность (технические науки) (2.3.6)

УДК 004.056:658.1:004.056.3:620.9
DOI: 10.24160/1993-6982-2023-5-182-189

Управление непрерывностью процессов на объектах критической информационной инфраструктуры в энергетике с позиций информационной безопасности

А.С. Минзов, А.Ю. Невский, М.А. Пасова

Обосновано введение нового механизма в систему управления информационной безопасностью (ИБ) для объектов критической информационной инфраструктуры (КИИ), основанного на обеспечении непрерывности процессов управления объектами энергетики. Существующее нормативно-правовое обеспечение информационной безопасностью КИИ не рассматривает механизмы обеспечения непрерывности процессов как комплексную систему восстановления КИИ при возникновении инцидентов информационной безопасности на объектах энергетики.

При проведении исследований использованы системный анализ для описания механизма непрерывности управления ИБ, теория рисков и ее приложения в сфере информационной безопасности, алгебра логики для описания условий и ограничений, при которых функционирует механизм непрерывности управления информационной безопасностью, теория нечетких множеств и величин для расчета показателей рисков обеспечения непрерывности системы защиты информации в объектах КИИ. Полученные результаты не противоречат существующим нормативным документам по защите КИИ и могут быть использованы для усиления защитных свойств объектов энергетики при появлении инцидентов ИБ, приводящих к остановке этих объектов. Эти решения являются экономически обоснованными.

Существующие нормативные документы по защите КИИ основаны на обеспечении конфиденциальности, целостности и доступности информации в информационных системах и слабо реагируют на возможность появления новых киберугроз, приводящих к остановкам производственных процессов, авариям и катастрофам. Возникает необходимость восстановления работы КИИ и системы их информационной безопасности в этих условиях. Это может быть успешно выполнено только при создании системы управления непрерывностью обеспечения защиты информации и ее восстановления после проведенных кибератак на АСУ.

Ключевые слова: управление непрерывностью бизнеса, критическая информационная инфраструктура, информационная безопасность, модель рисков.

Для цитирования: Минзов А.С., Невский А.Ю., Пасова М.А. Управление непрерывностью процессов на объектах критической информационной инфраструктуры в энергетике с позиций информационной безопасности // Вестник МЭИ. 2023. № 5. С. 182—189. DOI: 10.24160/1993-6982-2023-5-182-189.

Business Process Continuity Management at Critical Information Infrastructure Facilities in the Energy Sector from the Information Security Standpoint

A.S. Minzov, A.Yu. Nevskiy, M.A. Pasova

The article substantiates the introduction of a new mechanism into the information security (IS) management system for critical information infrastructure (CII) facilities. The proposed mechanism is based on ensuring the continuity of processes for managing power sector facilities. The existing regulatory framework supporting the CII information security does not consider the process continuity supporting mechanisms as an integrated CII recovering system in the event of information security jeopardizing incidents at energy sector facilities.

The studies were carried out using a system analysis for describing the IS management continuity mechanism, risk theory and its applications in the field of information security, logical algebra for describing the conditions and constraints under which the information security management continuity mechanism operates, and the theory of fuzzy sets and quantities for calculating indicators of risks connected with ensuring the information security system continuity at CII facilities.
The results obtained do not come in contradiction with the current regulatory documents on CII protection and can be used to improve the protective properties of energy facilities in the event of information security incidents that can cause their shutdown. These solutions are economically justified.
The existing regulatory documents for CII protection are based on ensuring the confidentiality, integrity and availability of information in information systems. However, they are poorly suited to cope with the possibility of new cyber threats to occur that may cause production process shutdowns, accidents, and disasters. Under these conditions, a need arises to recover the operation of the CII and their information security systems. This can only be done by setting up a system for managing the continuity of information security and recovering it after cyber attacks on the I&C.

Key words: business continuity management, critical information infrastructure, information security, risk model.

For citation: Minzov A.S., Nevskiy A.Yu., Pasova M.A. Business Process Continuity Management at Critical Information Infrastructure Facilities in the Energy Sector from the Information Security Standpoint. Bulletin of MPEI. 2023;5:182—189. (in Russian). DOI: 10.24160/1993-6982-2023-5-182-189.

Состояние вопроса

Интенсивное развитие высокотехнологической продукции, информационных технологий и систем коммуникаций в начале 2000-х гг. привело к массовому внедрению новых платформ информационных и автоматизированных систем управления технологическими и производственными процессами. Одновременно с этим возникли и требования к повышению безопасности данных систем, особенно к классифицируемым как значимые объекты критической информационной инфраструктуры (КИИ). К таким объектам относят: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, а также сети электросвязи, используемые для организации их взаимодействия и функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности [1]. Перечень объектов КИИ включает, как правило, непрерывные производства, остановка которых может привести к значительным негативным последствиям как на территории производственного объекта, так и в масштабах города, региона, государства и мира [2]. Таких примеров в мире много, а в России достаточно вспомнить аварию на Чернобыльской АЭС, когда при проведении эксперимента на 4-м энергоблоке по определению длительности «выбега» реактора после его остановки не были предусмотрены ситуации, приведшие практически к полному разрушению энергоблока и обширному радиоактивному загрязнению местности, последствия которого проявляются и сегодня. Подобные ситуации потребовали развития нормативно-правовой базы, позволяющей избежать подобных ситуаций за счет создания систем безопасности, а в случаях появления инцидентов без серьезных последствий восстанавливающей нарушенные процессы. Это направление обеспечения безопасности было определено как BCM (Business Continuity Management), что в России стало новым направлением проектирования систем безопасности, связанным с обеспечением непрерывности бизнеса. Понятие «непрерывность бизнеса» (Business Continuity) определяют как стратегическую и тактическую способность организации планировать свою работу в случае инцидентов и нарушения ее деятельности, направленной на обеспечение непрерывности деловых операций на установленном приемлемом уровне [3]. При этом, под термином «бизнес» подразумевают любые процессы, имеющие смысл.

Наибольшую известность по этому направлению обеспечения безопасности получили следующие международные и отечественные стандарты [3 — 8]. В отчете 2021 г. [9], выпущенном организацией BCI, приведена статистика использования стандарта ISO 22301. Результаты статистических данных показали, что почти половина опрошенных компаний используют рассматриваемый стандарт в качестве основы, но так и не имеют соответствующей сертификации по нему. Какие выгоды могут получить компании от сертификации по указанному стандарту? Из данных опроса следуте, что большинство организаций проходят сертификацию для повышения своей устойчивости, последовательного совершенствования и контроля процессов управления непрерывностью бизнеса, а также повышения экономической эффективности.

Ситуация с обеспечением непрерывности бизнеса объектов КИИ в России, на наш взгляд, требует значительно большего внимания. Это связано с тем, что в существующих нормативных документах [1, 10], определяющих требования к значимым объектам КИИ, понятие «непрерывность» не выделяется как отдельный критерий оценки их защищенности от киберугроз [11]. Вопросы восстановления КИИ после инцидентов рассматриваются в нормативных документах только как действия в нештатных ситуациях при эксплуатации значимого объекта КИИ [10]. При этом все действия ограничиваются только незначительным количеством рекомендуемых мер, не планируются заранее, не учитывается тот факт, что восстановление непрерывности

потребует совместных слаженных действий различных служб объектов КИИ. Считается, что для этого достаточно обеспечить такое свойство информации как «доступность», которое должно обеспечивать доступ к информации по запросу авторизованного субъекта. При этом совершенно не учитывается тот факт, что понятие «непрерывность» является более сложным и включает кроме свойства «доступность» еще и реакцию системы информационной безопасности на непредвиденные киберугрозы умышленного характера и восстановление информационных систем и защиты информации после сбоев и прерываний. Существующие международные стандарты по информационной безопасности [3 — 8] включают механизмы обеспечения непрерывности бизнес-процессов как обязательные элементы защиты информации. При этом сам механизм обеспечения рассматривается с позиций информационной безопасности как циклический процесс Деминга PDCA (Plan-do-check-act). Такое разное отношение к понятию непрерывности бизнес-процессов связано, на наш взгляд, со следующими факторами.

1. Концепции защиты информации ФСТЭК основаны на классификации защищенности информационных систем на моделях актуальных угроз. При этом бизнес-процессы, как и объекты оценки их безопасности (информационные активы) не рассматриваются. В этом и нет необходимости, поскольку все информационные системы защищаются по требованиям соответствующего класса или уровня защищенности информационных систем. Это не позволяет планировать и реализовывать процессы обеспечения непрерывности бизнеса, относя их к функциям других служб и структур.

2. Для обеспечения непрерывности бизнес-процессов с точки зрения информационной безопасности необходимо оценить их риски, что в существующих концепциях ФСТЭК не рассматривается, хотя и не исключается совсем [10].

3. Обеспечение непрерывности бизнеса предполагает проведение предварительных мероприятий по созданию системы запасов оборудования, расходных материалов, технических средств, резервированию каналов коммуникаций и связи, обучению персонала, проведение тренировок и учений по восстановлению систем после инцидентов и других мероприятий [3 — 8]. Это позволяет при обработке рисков в концепции стандартов [12 — 14] часть их переводить в область принимаемых рисков при определенных условиях и одновременного создания для них системы восстановления информационных систем, если угрозы этих рисков будут реализованы. Такой подход существенно сократит затраты на реализацию систем информационной безопасности.

4. Практически все существующие системы защиты информации базируются на методах заблаговременного построения системы информационной безопасности по моделям угроз или рисков (превентивная защита информации). Однако в некоторых случаях создать такую систему либо невозможно, либо нерационально из-за различных массогабаритных, энергетических, экономических и других ограничений. В этих случаях при определенных условиях возможно создание систем управления информационной безопасностью, основанных на восстановлении функций ИС (АСУ) и системы их безопасности. По существу, такие системы работают по принципу «решение проблем по мере их поступления» (инцидентная модель информационной безопасности). Можно предположить, что подобная модель системы информационной безопасности найдет применение в условиях жестких ограничений, например, в условиях космоса, агрессивной внешней среды и в др. Отметим, что этот подход к понятию «непрерывность» в теории разработки систем управления информационной безопасностью в настоящее время не рассматривается.

Такое различие в понимании терминов «непрерывность» и «доступность» для КИИ является принципиальным и требует разработки модели описания данных процессов, методик и условий обеспечения непрерывного функционирования КИИ при возникновении инцидентов информационной безопасности.

Анализ существующих работ по проблеме восстановления непрерывного функционирования КИИ после инцидентов показал следующее.

Вопросы восстановления объектов энергосистем после кибератак рассматривали с позиций киберустойчивости энергосистем, характеризующейся способностью к их восстановлению [15]. Практически все предлагаемые защитные мероприятия определяли только с точки зрения уже известных технологий кибератак и встраивали в архитектуру информационной безопасности КИИ [16, 17]. По существу этот подход представляет собой ту же превентивную систему защиты информации с некоторыми дополнительными функциями архитектуры информационной системы в форме дублирования работы отдельных ее компонентов. Единственный элемент восстановления энергосистем предложен при неизвестной кибератаке в виде перехода на ручной режим управления энергосистемой. Описанная в [17] архитектура экспертной системы не решает задачу восстановления энергосистем при кибератаках «нулевого дня», так как не определяет правила поведения при этих ситуациях. Таким образом, существующие подходы к обеспечению киберустойчивости энергосистем, в целом, не обеспечивают работу КИИ после кибератак «нулевого дня», и это требует проведения дополнительного исследования.

Модель непрерывного функционирования КИИ с позиций информационной безопасности

Модели безопасности в современных концепциях создают либо на основе анализа угроз и последующего определения класса или уровня защищенности ин-

формационной системы [10, 18], либо на основе оценки рисков информационной безопасности [12 — 14]. Анализ угроз доступности информации, проведенный с использованием базы данных угроз ФСТЭК [19], показал, что непосредственно на информационные системы КИИ объектов энергетики воздействуют следующие основные угрозы [15]:

● УБИ. 140. Угроза приведения системы в состояние «отказ в обслуживании»;

● УБИ. 164. Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре.

Они реализуются через множество сценариев кибератак на КИИ, большая часть из которых, кроме известных уязвимостей, используют уязвимости «нулевого дня». Каждый сценарий реализации этих угроз требует определенного количества принимаемых мер защиты, которые вряд ли вообще возможно реализовать в полном объеме. В базе данных угроз [15] представлено более 150 угроз, связанных с одновременным нарушением конфиденциальности, целостности и доступности информации при различных сценариях применения тактик и техник проникновения в информационные системы КИИ через их уязвимости [16]. Следовательно, в любом случае появляются инциденты по доступности к информации. Отсюда возникает необходимость решения двух задач:

● создания комплексной системы защиты КИИ от кибератак, включающей превентивные, проактивные и активные методы защиты информации, обеспечивающие непрерывность функционирования КИИ;

● проектирования системы непрерывного функционирования КИИ после появления инцидентов ИБ за счет своевременного восстановления системы управления КИИ, подвергшейся кибератакам.

Следовательно, полная модель обеспечения непрерывности функционирования КИИ с позиций информационной безопасности S может быть представлена в следующем виде:

$$S = S_p \cap S_d \cap S_a \cap S_v, \qquad (1)$$

где S_p — система обеспечения доступности информации за счет предупреждения инцидентов на этапах раннего выявления и блокирования сценариев их реализации на основе анализа событий.

В настоящее время данная задача решается средствами проактивной защиты [20] путем обнаружения корреляций между событиями и их графического визуального анализа средствами SIEM (Security Information and Event Management) в центрах обработки данных (SOC — Security Information and Event Management). Уровень полной автоматизации обнаружения сценариев атак к настоящему времени пока еще не достигнут даже по известным кибератакам, а существующие логико-лингвистические модели описания угроз [21] мало применимы для формализованного описания и последующего поиска сценариев развития инцидентов. Решение этой задачи позволит значительно повысить эффективность системы проактивной защиты КИИ и снизит вероятность появления инцидентов информационной безопасности и прерывания технологических процессов в КИИ.

S_d — система заблаговременного реагирования на инциденты, связанные с нарушением конфиденциальности, целостности и доступности информации (превентивная защита). Для защиты персональных данных и служебной тайны эта система проектируется на основе требований нормативных документов ФСТЭК [1, 10, 18] и обеспечивает доступность информации при выполнении требований к технической защите КИИ в соответствии с определенным классом защищенности информационной системы. Для защиты других видов неконфиденциальной информации используют нормативные документы, соответствующие международным стандартам [12 — 14].

S_a — система обеспечения доступности информации на этапе активной защиты с использованием антивирусного ПО, систем IDS (Intrusion Detection System — система обнаружения вторжений) и IPS (Intrusion Prevention System — система предотвращения вторжений). Это эффективная система защиты КИИ от известного вредоносного кода.

S_v — система восстановления управления КИИ после инцидента информационной безопасности. Она создается заранее и включает в себя набор планируемых, реализуемых и поддерживаемых в постоянной готовности организационных и технических решений.

Остановимся более подробно на создании системы S_v. В основу планирования ее организации положена модель рисков восстановления системы управления КИИ и обеспечения ее информационной безопасности при следующих условиях:

$$\forall r_i, \left(r_i \in R\right), \left(\Delta\tau_0 \geq \Delta\tau_i\right) \rightarrow \left(r_i \in S_v\right), \qquad (2)$$

где r_i — значение риска обеспечения непрерывности, при котором восстановление нарушенных отдельных процессов не вызывает недопустимых по длительности Δt_i их прерываний; $\Delta\tau_0$ — предельное значение времени прерывания процессов, при котором не проявляются негативные последствия остановки; $\Delta\tau_i$ — время восстановления системы управления и информационной безопасности после инцидента.

С учетом требований стандарта [7] модель рисков R восстановления системы КИИ и ее информационной безопасности выглядит так:

$$R = \left\{t_i, a_i^k, r_i, \Delta\tau_i, \left\{c_{ij}\right\}, z_i\right\}, \qquad (3)$$

где t_i — угроза, приводящая к инциденту информационной безопасности для КИИ и прерыванию его деятельности; a_i^k — критичный информационный актив и его ценность в принятой системе метрик (k определяет отношение к этому активу как к возможной цели кибератаки), нарушение деятельности актива может

привести к негативным последствиям для КИИ после инцидента информационной безопасности; r_i — величина предотвращенного ущерба в принятой системе метрик при восстановлении системы управления КИИ; $\{c_{ij}\}$ — меры по восстановлению непрерывности (количество мер j может быть несколько для i-го риска), выбираемые такими, чтобы выполнялось условие (2); z_i — общие затраты на обработку i-го риска.

Рассмотренная модель рисков (3) несколько отличается от других моделей [7, 13, 22], так как не использует фактор уязвимостей информационных активов. В ее основу положены критические информационные активы, воздействие инцидентов информационной безопасности на которые ведет к негативным последствиям КИИ и прерыванию его деятельности. Для оценки рисков можно использовать следующие правила выбора целей умышленных атак на системы управления КИИ:

- цель кибератак — наиболее критичные информационные активы, вывод из строя которых приводит к появлению значительных политических, социальных, экономических и экологических последствий [18];
- цель кибератак — информационные активы, вывод из строя которых требует значительных усилий и времени по восстановлению системы управления КИИ и информационной безопасности.

$$\forall a_i,\left(a_i \in A\right),\left(r_{\max} \le r_i\right),\left(\Delta\tau_i \gg \Delta\tau_0\right). \qquad (4)$$

Модель, подобная (3), ориентированная на восстановление системы управления КИИ после инцидентов, можно использовать и в других концепциях создания систем управления информационной безопасностью КИИ. В этом случае управление рисками проходит с учетом факторов угроз и уязвимостей v_i:

$$R = \left\{t_i, a_i, v_i, r_i, \Delta\tau_i, c_i\ , z_i\right\}. \qquad (5)$$

Параметры (t_i, a_i^k, r_i) в модели (3) и (t_i, a_i, v_i, r_i) в модели (5) оцениваются методом нечетких множеств [23, 24]. Параметры задаются в форме лингвистических переменных, каждая из которых определяется соответствующим множеством нечетких переменных (термов) в заданных интервалах и функциями принадлежности. Блок правил обработки рисков конструируется из условий:

- значения рисков увеличиваются с возрастанием ценности информационных активов, величины уязвимости системы и меры опасности угрозы;
- уровень доверия к правилу возрастает на границах интервала риска.

Определение параметров риска r_i происходит после процедуры дефазификации. Погрешности оценки каждого риска зависят от количества термов в лингвистических переменных, корректности и непротиворечивости блока правил, вида и параметров функции принадлежности.

Моделирование относительной погрешности оценки суммарного значения рисков R показало, что распределение этих оценок подчиняется нормальному закону распределения случайных величин и, в значительной степени, зависит от количества рисков n.

При размере матрицы рисков, равном 50, максимальное значение погрешности не превышает ±10%. С уменьшением количества рисков погрешность увеличивается до 30% (при n = 10). Это утверждение согласуется с центральной предельной теоремой, которая утверждает, что сумма достаточно большого количества слабо зависимых случайных величин, имеющих примерно одинаковые масштабы (ни одно из слагаемых не доминирует и не вносит в сумму определяющего вклада), имеет распределение, близкое к нормальному. Устойчивость этих оценок зависит от статистики случайных величин показателей для каждого риска, степени независимости рисков и количества обрабатываемых рисков.

Для устранения возможности переоценки значений рисков при одновременном воздействии на активы нескольких угроз используют процедуру коррекции суммарного значения риска и отдельных рисков [21].

Для оценки суммарных значений затрат Z служат реальные значения стоимости технических средств защиты информации других затрат. При этом должна быть обязательно исключена возможность повторного использования технических средств защиты для разных рисков.

Этапы планирования непрерывности функционирования КИИ с позиций информационной безопасности

В соответствии с требованиями нормативных документов [7, 14], каждая организация обязана обеспечить непрерывность информационной безопасности в процессах управления непрерывностью бизнеса и восстановления системы после инцидентов. С этой целью должны быть разработаны соответствующие планы и процедуры реагирования на инциденты и восстановление нарушенных процессов защиты информации. В основе этих документов положен план обработки рисков непрерывности информационной безопасности для КИИ по моделям (3), (5). Для этого необходимо:

1) определить исходные данные, относящиеся к контексту организации D: устав, структуру КИИ, технологии и процессы сбора и обработки информации, АСУ и АСУТП, существующую архитектуру системы информационной безопасности и ее размещение, информационные активы, результаты аудита информационной безопасности КИИ;

2) проанализировать критичность информационных активов для обеспечения непрерывности бизнес-процессов по условиям () и оценить параметр $\Delta\tau_0$.

3) провести оценку рисков непрерывности информационной безопасности (3) и выбор мер контроля и управления при выполнении условия (2). Возможны и иные подходы к оценке риска [23, 24];

4) оценить затраты на меры контроля и управления z_i;

5) оценить общие затраты и выбрать вариант восстановления по заданным критериям или ограничениям;

6) ввести ссылки на процедуры восстановления риска и ответственных за их выполнение, а описание процедур восстановления в приложениях к плану в план обработки рисков;

7) повторить действия по оценке очередных рисков с п. 2;

8) оценить эффективность планирования непрерывности информационной безопасности.

Заключение

Тенденции увеличения количества и сложности сценариев реализации киберугроз в отношении КИИ потребовали совершенствования существующей нормативно-правовой базы, позволяющей не только предупреждать и активно реагировать на события, приводящие к инцидентам, но и восстанавливать нарушенные процессы на объектах энергетики. Это и определило цель исследования — разработку механизма управления информационной безопасностью для объектов КИИ, основанного на обеспечении непрерывности процессов управления объектами энергетики путем планирования и восстановления систем управления ИБ при возникновении инцидентов информационной безопасности. Существующие нормативные документы по защите КИИ основаны на обеспечении конфиденциальности, целостности и доступности информации в информационных системах и слабо реагируют на возможность появления новых киберугроз, приводящих к остановкам производственных процессов, авариям и катастрофам. Возникает необходимость восстановления работы КИИ и системы их информационной безопасности в этих условиях. Это может быть успешно выполнено только при создании системы управления непрерывностью обеспечения защиты информации и ее восстановления после проведенных кибератак на АСУ.

Полученные результаты не противоречат существующим нормативным документам по защите КИИ и могут быть использованы для усиления защитных свойств объектов энергетики при появлении инцидентов ИБ, приводящих к остановке этих объектов. Данные решения являются экономически обоснованными.

Выводы

Существующие нормативные документы по защите КИИ основаны на обеспечении конфиденциальности, целостности и доступности информации в информационных системах и слабо реагируют на возможность появления новых киберугроз, приводящих к остановкам производственных процессов, авариям и катастрофам. Возникает необходимость восстановления работы КИИ и системы их информационной безопасности в этих условиях, что может быть успешно выполнено только при создании системы управления непрерывностью обеспечения защиты информации и ее восстановления после проведенных кибератак на АСУ.

Литература

1. **Федеральный** закон № 187-ФЗ от 26 июля 2017 г. «О безопасности критической информационной инфраструктуры РФ».

2. **Постановление** Правительства РФ № 127 от 08 февраля 2018 г. «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».

3. **ГОСТ Р 53647.3—2015.** Менеджмент непрерывности бизнеса. Ч. 3. Руководство по обеспечению соответствия требованиям ГОСТ Р ИСО 22301.

4. **ISO 22301:2012.** Societal Security — Business Continuity Management Systems — Requirements.

5. **ISO/IEC 27031:2011.** Information Technology — Security Techniques — Guidelines for Information and Communication Technology Readiness for Business Continuity.

6. **NIST SP 800-34 Rev. 1.** Contingency Planning Guide for Federal Information Systems.

7. **ГОСТ Р ИСО/МЭК 27031—2012.** Информационная технология. Методы и средства обеспечения

References

1. **Federal'nyy** Zakon № 187-FZ ot 26 Iyulya 2017 g. «O bezopasnosti Kriticheskoy Informatsionnoy Infrastruktury RF». (in Russian).

2. **Postanovlenie** Pravitel'stva RF № 127 ot 08 Fevralya 2018 g. «Ob Utverzhdenii Pravil Kategorirovaniya Ob'ektov Kriticheskoy Informatsionnoy Infrastruktury Rossiyskoy Federatsii, a Takzhe Perechnya Pokazateley Kriteriev Znachimosti Ob'ektov Kriticheskoy Informatsionnoy Infrastruktury Rossiyskoy Federatsii i Ikh Znacheniy». (in Russian).

3. **GOST R 53647.3—2015.** Menedzhment Nepreryvnosti Biznesa. Ch. 3. Rukovodstvo po Obespecheniyu Sootvetstviya Trebovaniyam GOST R ISO 22301. (in Russian).

4. **ISO 22301:2012.** Societal Security — Business Continuity Management Systems — Requirements.

5. **ISO/IEC 27031:2011.** Information Technology — Security Techniques — Guidelines for Information and Communication Technology Readiness for Business Continuity.

6. **NIST SP 800-34 Rev. 1.** Contingency Planning Guide for Federal Information Systems.

7. **GOST R ISO/MEK 27031—2012.** Informatsionnaya Tekhnologiya. Metody i Sredstva Obespecheniya

безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.

8. **ГОСТ Р ИСО 22301—2014.** Системы менеджмента непрерывности бизнеса. Общие требования.

9. **BCI** Horizon Scan Rep. 2021 [Электрон. ресурс] https://www.bsigroup.com/globalassets/localfiles/en-th/iso-22301/bci-horizon-scan-report/bci-horizon-scan-report-2021-th.pdf (дата обращения 31.01.2023).

10. **Приказ** ФСТЭК России № 239 от 25 декабря 2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

11. **Минзов А.С.** О новой номенклатуре научных специальностей и не только // Вопросы кибербезопасности. 2022. №. 2(48). С. 2—4.

12. **ГОСТ Р ИСО/МЭК 27001—2006.** Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

13. **ГОСТ Р ИСО/МЭК 27005—20012.** Информационная технология. Методы и средства обеспечения информационной безопасности. Менеджмент риска информационной безопасности.

14. **ГОСТ Р ИСО/МЭК 27002—2012.** Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

15. **Воропай Н.И. и др.** Проблемы развития цифровой энергетики в России // Проблемы управления. 2019. № 1. С. 2—14.

16. **Колосок И.Н., Коркина Е.С.** Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. 2019. №. 3(15). С. 121—131.

17. **Гаськова Д.А., Массель А.Г.** Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры // Вопросы кибербезопасности. 2019. № 2(30). С. 42—49.

18. **Методика** оценки угроз безопасности информации [Электрон. ресурс] https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=lms2gm69hr577050030 (дата обращения 31.01.2023).

19. **Банк** данных угроз ФСТЭК [Электрон. ресурс] https://bdu.fstec.ru/ (дата обращения 22.09.2022).

20. **Минзов А.С., Баронов О.Р., Минзов С.А., Осипов П.А.** Управление событиями информационной безопасности. М.: ВНИИгеосистем, 2020.

21. **Язов Ю., Соловьев С.В., Тарелкин М.А.** Логико-лингвистическое моделирование угроз безопасности информации в информационных системах // Вопросы кибербезопасности. 2022. №. 4. С. 13—25.

Bezopasnosti. Rukovodstvo po Gotovnosti Informatsionno-kommunikatsionnykh Tekhnologiy k Obespecheniyu Nepreryvnosti Biznesa. (in Russian).

8. **GOST R ISO 22301—2014.** Sistemy Menedzhmenta Nepreryvnosti Biznesa. Obshchie Trebovaniya. (in Russian).

9. **BCI** Horizon Scan Rep. 2021 [Elektron. Resurs] https://www.bsigroup.com/globalassets/localfiles/en-th/iso-22301/bci-horizon-scan-report/bci-horizon-scan-report-2021-th.pdf (Data Obrashcheniya 31.01.2023).

10. **Prikaz** FSTEK Rossii № 239 ot 25 Dekabrya 2017 g. «Ob Utverzhdenii Trebovaniy po Obespechniyu Bezopasnosti Znachimykh Ob'ektov Kriticheskoy Informatsionnoy Infrastruktury Rossiyskoy Federatsii». (in Russian).

11. **Minzov A.S.** O Novoy Nomenklature Nauchnykh Spetsial'nostey i ne Tol'ko. Voprosy Kiberbezopasnosti. 2022;2(48):2—4. (in Russian).

12. **GOST R ISO/MEK 27001—2006.** Informatsionnaya Tekhnologiya. Metody i Sredstva Obespecheniya Bezopasnosti. Sistemy Menedzhmenta Informatsionnoy Bezopasnosti. (in Russian).

13. **GOST R ISO/MEK 27005—20012.** Informatsionnaya Tekhnologiya. Metody i Sredstva Obespecheniya Informatsionnoy Bezopasnosti. Menedzhment Riska Informatsionnoy Bezopasnosti. (in Russian).

14. **GOST R ISO/MEK 27002—2012.** Informatsionnaya Tekhnologiya. Metody i Sredstva Obespecheniya Bezopasnosti. Svod Norm i Pravil Menedzhmenta Informatsionnoy Bezopasnosti. (in Russian).

15. **Voropay N.I. i dr.** Problemy Razvitiya Tsifrovoy Energetiki v Rossii. Problemy Upravleniya. 2019;1:2—14. (in Russian).

16. **Kolosok I.N., Korkina E.S.** Analiz Kiberbezopasnosti Tsifrovoy Podstantsii s Pozitsiy Kiberfizicheskoy Sistemy. Informatsionnye i Matematicheskie Tekhnologii v Nauke i Upravlenii. 2019;3(15):121—131. (in Russian).

17. **Gas'kova D.A., Massel' A.G.** Tekhnologiya Analiza Kiberugroz i Otsenka Riskov Narusheniya Kiberbezopasnosti Kriticheskoy Infrastruktury. Voprosy kiberbezopasnosti. 2019;2(30):42—49. (in Russian).

18. **Metodika** Otsenki Ugroz Bezopasnosti Informatsii [Elektron. Resurs] https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya (in Russian).-2021-g?ysclid=lms2gm69hr577050030 (Data Obrashcheniya 31.01.2023).

19. **Bank** Dannykh Ugroz FSTEK [Elektron. Resurs] https://bdu.fstec.ru/ (Data Obrashcheniya 22.09.2022). (in Russian).

20. **Minzov A.S., Baronov O.R., Minzov S.A., Osipov P.A.** Upravlenie Sobytiyami Informatsionnoy Bezopasnosti. M.: VNIIgeosistem, 2020. (in Russian).

21. **Yazov Yu., Solov'ev S.V., Tarelkin M.A.** Logiko-lingvisticheskoe Modelirovanie Ugroz Bezopasnosti Informatsii v Informatsionnykh Sistemakh. Voprosy Kiberbezopasnosti. 2022;4:13—25. (in Russian).

22. **Минзов А.С., Невский А.Ю., Баронов О.Р.** Управление рисками информационной безопасности. М.: ВНИИгеосистем, 2019.

23. **Большаков А.С, Жила А.И., Осин А.В.** Управление информационной безопасностью персональных данных с использованием нечеткой логики // Наукоемкие технологии в космических исследованиях Земли. 2021. № 4. С. 37—47.

24. **Дорофеев А.В., Марков А.С.** Планирование обеспечения непрерывности бизнеса и восстановления // Вопросы кибербезопасности. 2015. №. (11). С. 68—73.

22. **Minzov A.S., Nevskiy A.Yu., Baronov O.R.** Upravlenie Riskami Informatsionnoy Bezopasnosti. M.: VNIIgeosistem, 2019. (in Russian).

23. **Bol'shakov A.S, Zhila A.I., Osin A.V.** Upravlenie Informatsionnoy Bezopasnost'yu Personal'nykh Dannykh s Ispol'zovaniem Nechetkoy Logiki. Naukoemkie Tekhnologii v Kosmicheskikh Issledovaniyakh Zemli. 2021; 4:37—47. (in Russian).

24. **Dorofeev A.V., Markov A.S.** Planirovanie Obespecheniya Nepreryvnosti Biznesa i Vosstanovleniya. Voprosy Kiberbezopasnosti. 2015;(11):68—73. (in Russian).

Сведения об авторах:

Минзов Анатолий Степанович — доктор технических наук, профессор кафедры безопасности и информационных технологий НИУ «МЭИ», e-mail: MinsovAS@mpei.ru
Невский Александр Юрьевич — кандидат технических наук, директор инженерно-экономического института, заведующий кафедрой безопасности и информационных технологий НИУ «МЭИ», e-mail: NevskyAY@mpei.ru
Пасова Майя Алексеевна — магистрант кафедры безопасности и информационных технологий НИУ «МЭИ», e-mail: pasovama@mpei.ru

Information about authors:

Minzov Anatoliy S. — Dr.Sci. (Techn.), Professor of Security and Information Technologies Dept., NRU MPEI, e-mail: MinsovAS@mpei.ru
Nevskiy Aleksandr Yu. — Ph.D. (Techn.), Director of Engineering-economic Institute, Head of Security and Information Technologies Dept., NRU MPEI, e-mail: NevskyAY@mpei.ru
Pasova Maya A. — Master's Student of Security and Information Technologies Dept., NRU MPEI, e-mail: pasovama@mpei.ru

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов
Conflict of interests: the authors declare no conflict of interest

Статья поступила в редакцию: *11.12.2022*
The article received to the editor: *11.12.2022*

Статья принята к публикации: *06.06.2023*
The article has been accepted for publication: *06.06.2023*