ИССЛЕДОВАНИЕ МЕТОДИК КОНТРОЛЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Лившиц И.И.[1], Бакшеев А.С.[2]

Целью работы *является анализ существующих практик выполнения анализа защищенности и аудита ИБ (NIST, OWASP, Cobit, OSSTMM, PTES и ГОСТ Р ИСО/МЭК), применяемых для получения объективных и достоверных данных для формирования оперативных оценок защищенности объектов КИИ и разработка модели аудита ИБ для объектов КИИ.*

Метод исследования: *для достижения цели работы применялись методы анализа и структурной декомпозиции из теории системного анализа, выявление признаков, существенных для оптимизации процесса аудита ИБ для объектов КИИ.*

Результат исследования: *в работе представлен детальный анализ и сопоставление существующих лучших практик выполнения анализа защищенности и аудита информационной безопасности (NIST, OWASP, Cobit, OSSTMM, PTES и ГОСТ Р ИСО/МЭК), применяемых для получения оценок защищенности объектов КИИ. Сделаны выводы о возможных направлениях оптимизации процесса аудита ИБ для объектов КИИ. Представлена модель аудита ИБ для объектов КИИ, отличающаяся «двойным» режимом реализации полного цикла обеспечения безопасности объектов КИИ.*

Научная новизна *заключается в разработке модели аудита ИБ для объектов КИИ, отличающаяся возможностью «двойного» режима для полного цикла обеспечения безопасности объектов КИИ – полного национального режима и комбинированного режима, который позволяет при необходимости включать дополнительные функциональные блоки.*

Ключевые слова: *угрозы, уязвимости, стандарт, риск, аудит, меры защиты, информационная безопасность, NIST, OWASP, Cobit, OSSTMM, PTES, ISSAF.*

DOI:10.21681/2311-3456-2022-6-40-52

Введение

В 2018 г. вступил в силу Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и проблема обеспечения безопасности объектов КИИ получила формальный государственный статус. Игнорирование своевременного и соразмерного внедрения комплекса мер по защите на объектах КИИ может привести к серьёзным инцидентам, известные примеры в области топливно-энергетического комплекса (далее – ТЭК): нефтяной терминал SaudiAramco[3], нефтяной завод Oil India[4], нефтеперерабатывающий завод Petro Rabigh[5], трубопровод Colonial Pipeline[6] и др. Актуальность проблемы защиты объектов КИИ не вызывает сомнения, и для снижения ущерба и минимизации рисков возникает необходимость создания экономически эффективной и функционально полной системы безопасности объектов КИИ.

Дополнительно отметим, что необходимость защиты объектов КИИ отмечается в системе документов Российской Федерации, например:

— в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646;

3 https://www.kommersant.ru/doc/4584906?

4 https://www.securitylab.ru/news/531297.php

5 https://www.securitylab.ru/analytics/523661.php

6 https://www.securitylab.ru/news/523424.php

1 Лившиц Илья Иосифович, доктор технических наук, профессор практики Университета ИТМО, Санкт-Петербург, Россия. E-mail: Livshitz.il@yandex.ru

2 Бакшеев Андрей Сергеевич, магистрант группы N41532c Университета ИТМО, Санкт-Петербург, Россия. E-mail: Baksheev.Andrey@yandex.com

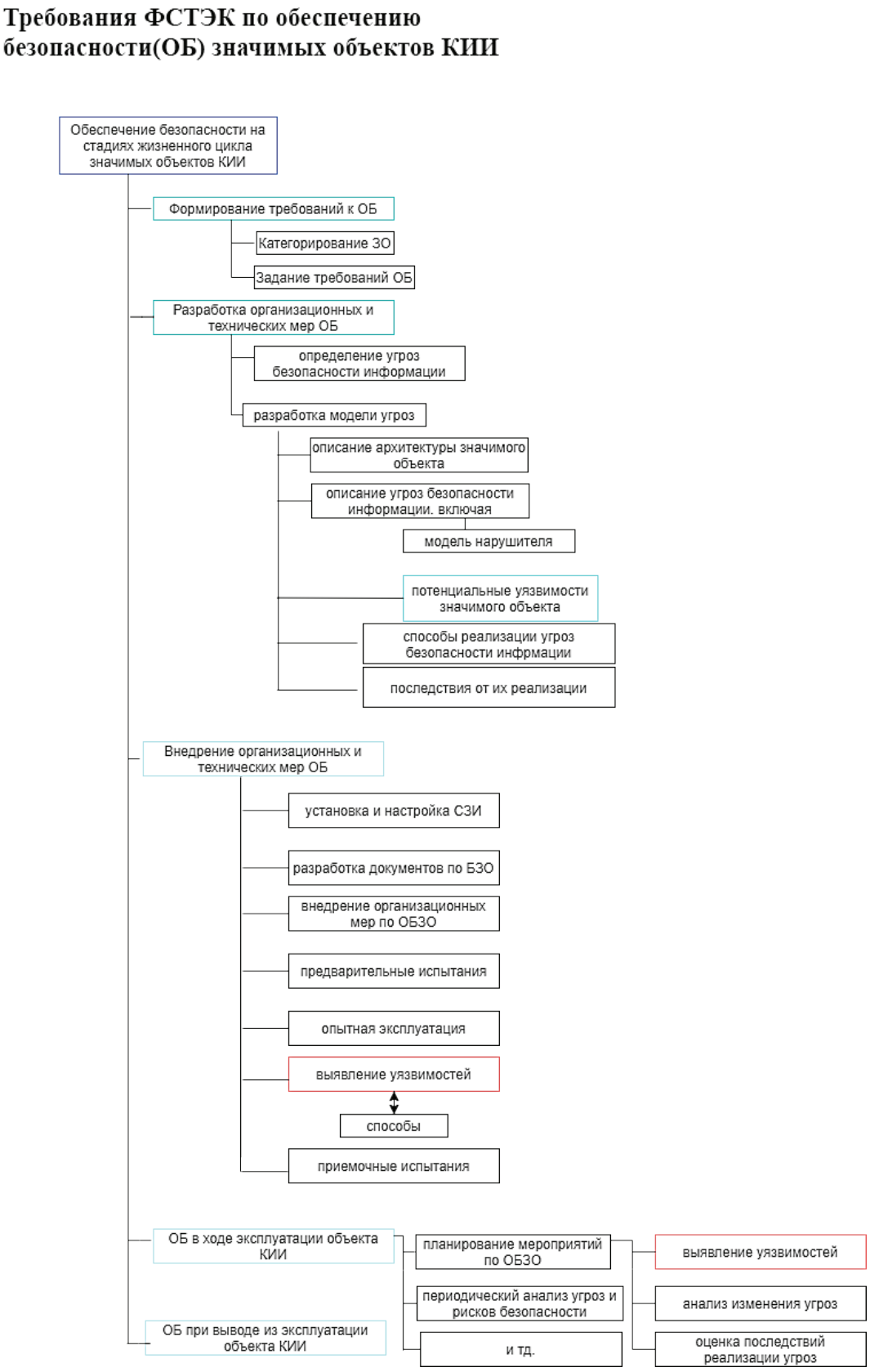

Рис. 1. Структурная модель требований ФСТЭК по обеспечению ИБ объектов КИИ

— в «Стратегии национальной безопасности Российской Федерации», утвержденной Указом Президента РФ от 02.07.2021 № 400;
— в Постановлении Правительства Российской Федерации 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».

Имеющиеся уязвимости в компонентах, а также нерациональный выбор мер защиты могут привести к отказу собственных систем и вызвать нарушение режимов критических процессов и функционирования объектов КИИ, что особенно важно для объектов ТЭК. Поэтому важно признавать актуальность данной проблемы и обеспечить в полном жизненном цикле функционирования объектов КИИ детальный и непрерывной анализ и оценку рисков (остаточных рисков). В соответствии с лучшим практиками в полный процесс анализа и оценки рисков входит идентификация уязвимостей, оценка вероятности возникновения угроз и анализ (аудит) текущего уровня защищенности объектов КИИ. В данном процессе необходимо не только выявить уязвимости и определить угрозы, но и своевременно и точно определить риски ИБ для объектов КИИ и обеспечить полный замкнутый цикл контроля защищенности для применения наиболее эффективных мер защиты [1,2].

Актуальность исследования заключается в необходимости исследования доступных методик для контроля текущего уровня защищенности информации на объектах КИИ, основанных на использовании процедур аудита ИБ и тестирования на проникновение в рамках полного цикла обеспечения ИБ.

Объектом исследования является контроль текущего уровня защищенности информации на объектах КИИ.

Предметом исследования является методика контроля уровня защищенности информации на объектах КИИ.

Вербальная постановка задачи

Дано: *известные практики выполнения анализа защищенности и аудита ИБ (NIST, OWASP, Cobit, OSSTMM, PTES и ГОСТ Р ИСО/МЭК);*

Необходимо: *провести анализ известных практик анализа защищенности и предложить новую модель аудита ИБ, обладающую оптимальными характеристиками для соответствия требованиями безопасности для объектов КИИ.*

Исходные данные: *требования для обеспечения безопасности объектов КИИ в Российской Федерации.*

Ограничения: *состав мер защиты для объектов КИИ, определенный ФСТЭК; известные ограничения формального процесса аудита ИБ; функциональные ограничения компонентов объектов КИИ; ограничения временных и стоимостных ресурсов для аудитов ИБ.*

Задачи исследования определены следующим образом:

— изучение существующей нормативной базы и лучших международных стандартов;
— рассмотрение подходов при выборе мер защиты КИИ;
— исследование существующих стандартов аудита ИБ;
— построение модели проведения контроля защищенности для объектов КИИ;
— выбор оптимальных мер по обеспечению безопасности объектов КИИ.

Часть 1. Требования обеспечения информационной безопасности для объектов КИИ

1. ФСТЭК России

В Российской Федерации требования обеспечения ИБ для объектов КИИ, помимо указанных выше, установлены в приказах ФСТЭК России № 235 от 21.12.2017 г. «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» и № 239 от 25.12.2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Структурная модель требований ФСТЭК по обеспечению безопасности значимых объектов КИИ представлена на рис. 1.

В мировой практике применяется несколько методик и стандартов, которые могут быть приняты в качестве лучших практик для контроля уровня защищенности на объектах КИИ. Рассмотрим далее кратко их основные особенности.

2. Control Objectives for Information and Related Technologies (COBIT)

COBIT представляет собой методологию управления ИТ, которую разрабатывает некоммерческая

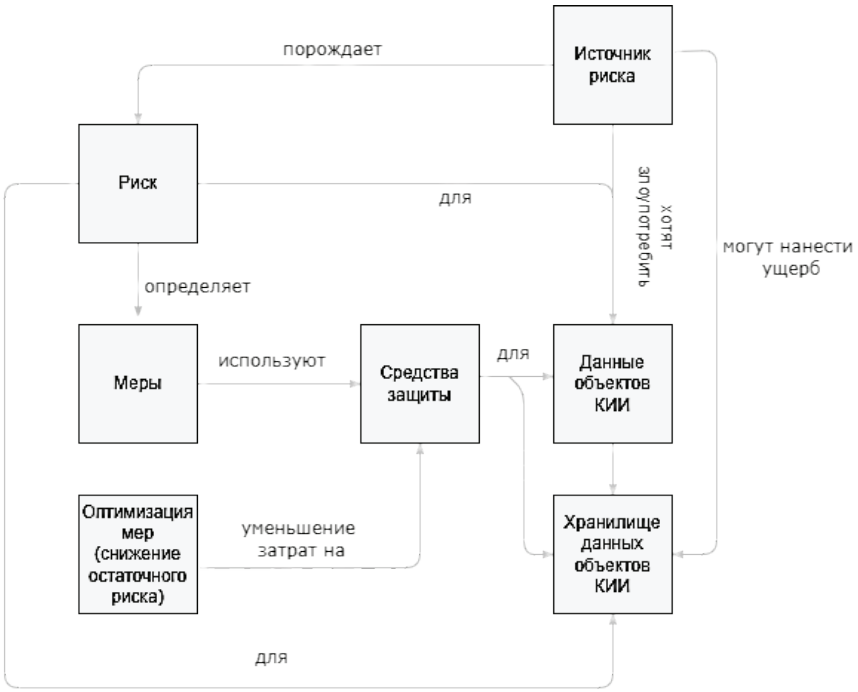

Рис.2. Схема, отражающая место риска ИБ для защиты объектов КИИ

организация Information Systems Audit and Control Association (ISACA). На данный момент стандарт COBIT 2019 состоит из 4 базовых комплектов [3, 4, 5]:

- Введение и методология (Framework: Introduction and Methodology);
- Цели управления и менеджмента (Framework: Governance and Management Objectives);
- Руководство по проектированию: Проектирование решений по управлению информацией и технологиями; (Design Guide: Designing an Information and Technology Governance Solution);
- Руководство по внедрению: внедрение и оптимизация решения по управлению информацией и технологиями. (Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution).

Для целей данной публикации важно, что издана дополнительная часть: «Внедрение основ кибербезопасности NIST с использованием COBIT 2019» (Implementing the NIST cybersecurity framework using COBIT 2019). С учетом фокуса на раздельное управление (*Management*) и руководство (*Governance*), необходимо принять во внимание каскад целей COBIT, в котором явно определены цели согласования (как ИТ-цели) и цели (как факторы влияния). Среди наиболее важных факторов влияния авторы полагают возможным ранжировать по приоритетам:

- процессы (набор практик и действий для достижения определенных результатов);
- организационные структуры (субъекты принятия решений на предприятии);
- услуги, инфраструктура и приложения (включают в себя инфраструктуру, технологии и приложения на предприятии);
- информация, распространяемая на предприятии;
- культура, этика и поведение работников;
- люди, навыки и компетенции (необходимые для принятия правильных решений).

Для целей данной публикации крайне важно, что в рамках COBIT функции аудита ИБ заключаются в мероприятиях, направленных на контроль уровня защищенности на объектах КИИ. Допускаются следующие форматы проверок:

- оценка уровней зрелости процессов;
- оценка уровней возможностей процессов;
- оценка результативности и эффективности контролей;
- соответствие регламентам (стандартам).

3. ГОСТ Р ИСО/МЭК серии 27000

Международные стандарты ISO/IEC (национальные стандарты ГОСТ Р ИСО/МЭК) серии 27000 являются широко распространёнными, поскольку

Рис. 3. Оценка рисков ИБ при эксплуатации объектов КИИ в нотации IDEF0

содержат согласованные мировым экспертным сообществом практики обеспечения ИБ. Для целей данной публикации авторы рекомендуют для контроля уровня защищенности на объектах КИИ выбрать следующее:

- разработать стратегию управления рисками объектов КИИ;
- определение (категорирование) объектов КИИ, которые подвержены угрозам и атакам, с целью применения мер по снижению рисков до приемлемого уровня;
- проверка (аудит) применяемых мер и средств защиты с учетом категории объекта;
- повышение осведомленности персонала о кибербезопасности.

Объект КИИ в нотации ГОСТ Р ИСО/МЭК серии 27000 рассматривается как актив с последующим детальным анализам имеющихся уязвимостей, возможных угроз и оцениванием рисков нарушения известных свойств ИБ – конфиденциальности, целостности и доступности. Оценка рисков (определяемых для базового состояния актива) и остаточных рисков (определяемых после внедрения в рамках систем обеспечения безопасности комплекса мер и средств защиты) является важным процессом в общей практике обеспечения ИБ.

Представим на рис. 2 схему, отражающую место менеджмента риска ИБ в рамках задачи контроля уровня защищенности на объектах КИИ.

Оценка риска ИБ при эксплуатации объектов КИИ представлена на рис. 3.

Как показано на рис. 3, процесс оценки рисков при эксплуатации объектов КИИ заключается в определении бизнес-процессов предприятия и активов, которые имеют определенную ценность. На основе известных требований к обеспечению безопасности объектов КИИ, необходимо оценить риски (остаточные риски) для оценки уже внедрённых меры защиты и необходимость пересмотра новых (перспективных) мер защиты[7]. Более детально процесс оценки рисков для объекта КИИ в нотации IDEF0 показан на рис. 4. Основной фокус сделан на объективное определение рисков, оценивание остаточных рисков и последующий пересмотр мер защиты – обеспечение полного жизненного цикла управления (цикла PDCA), как было отмечено выше.

Аудит ИБ в соответствии с требованиями стандартов ГОСТ Р ИСО/МЭК серии 27006 и 27007 включает в себя следующие этапы:

- проведение оценки рисков, связанных с вероятностью реализации угроз ИБ в отношении объектов КИИ;
- оценку текущего состояния объектов КИИ;
- оценку соответствия объектов КИИ существующим стандартам в области ИБ;

7 Оценка рисков при построении защиты объектов критической информационной инфраструктуры – [Электронный ресурс]. – Режим доступа: https://safe-surf.ru/specialists/article/5287/666251/ (дата обращения: 29.06.2022).

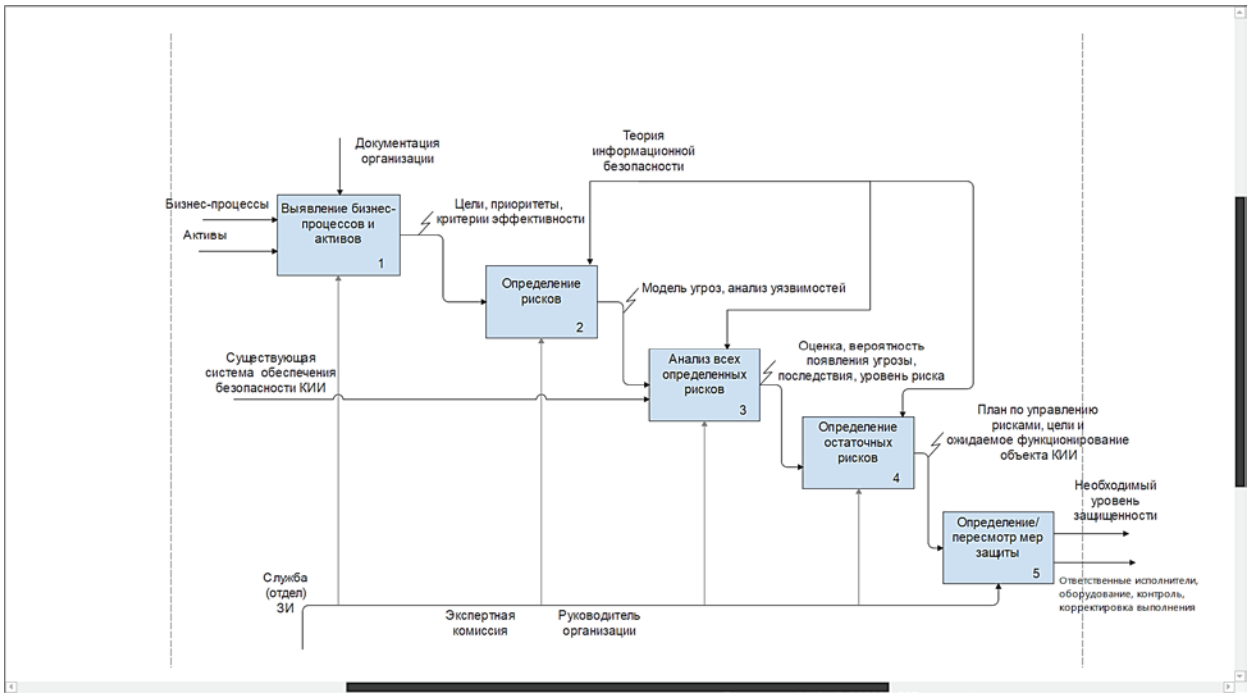

Рис. 4. Процесс оценки рисков (остаточных рисков) в нотации IDEF0

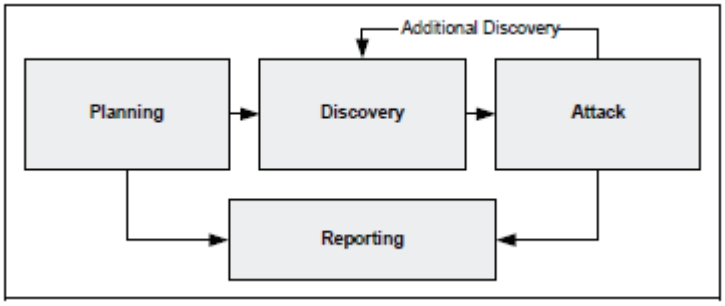

Рис. 5. Этапы тестирования

— выработку рекомендаций по повышению эффективности защиты объектов КИИ.

Отметим применимые виды аудитов ИБ для объектов КИИ:

— экспертный аудит ИБ (выявление уязвимостей существующих мер защиты на основе опыта экспертов);
— оценка соответствия установленных требований (*Compliance*);
— инструментальный анализ защищенности объекта защиты (*Penetration test*);
— комплексный аудит, включающий все применимые методы.

Часть 2. Методики для контроля уровня защищенности объектов КИИ

Как изложено выше, комплексный аудит ИБ является более широким и объемлющим системным мероприятием, чем тестирование на проникновение. Рассмотрим далее известные методики контроля уровня защищённости, в том числе – тестирование на проникновение.

1. NIST SP 800-115 Technical Guide to Information Security Testing and Assessment

Стандарт National Institute of Standards and Technology описывает порядок проведения тестирования на проникновение, рекомендации по анализу полученных результатов и разработке мер по обра-

ботке рисков [6 – 9]. Стандарт разработан и поддерживается центром по компьютерной безопасности Computer Security Resource Center (CSRC) – подразделение национального института стандартизации США National Institute of Standards and Technology (NIST) [8]. Разделы стандарта включают следующее:

- обзор тестирования и экспертизы безопасности;
- обзор методов;
- определение цели и техники анализа;
- техники оценки уязвимостей объектов;
- планирование оценки безопасности;
- выполнение оценки безопасности;
- пост-тестовые мероприятия.

Типовой тест на проникновение состоит из следующих этапов (рис. 5):

- планирование (*Planning*);
- исследование (*Discovery*);
- атака (*Attack*);
- отчёт (*Reporting*).

Стандарт рекомендует проводить тестирование на проникновение в следующих случаях:

- определение защищенности и устойчивости функционирования объекта к реально существующим информационно-техническим воздействиям (ИТВ);
- определение трудоемкости преодоления периметра защиты объекта;
- выявление уязвимостей существующих мер и средств защиты объекта;
- определение способности системы защиты объекта своевременно обнаруживать ИТВ;
- реагирование на ИТВ системы защиты объекта.

Для целей данной публикации важно, что указанный стандарт предоставляет несколько шаблонов для тестирования стандартных функций обеспечения и мер защиты ИБ, что может быть применено на многих типовых объектах ТЭК.

2. Open Source Security Testing Methodology Manual (OSSTMM)

Методика «The Open Source Security Testing Methodology Manual» (OSSTMM) разработана институтом Institute for Security and open Methodologies (ISECOM). Методика OSSTMM содержит подробный план тестирования, метрики для оценки уровня безопасности и рекомендации по отчёту[9]. Для тестирования определены 5 каналов и для полного аудита безопасности требуется тестирование всех каналов:

- человек (человеческий элемент общения);
- физическая безопасность (материальный элемент безопасности);
- беспроводная связь (безопасность электронных коммуникаций);
- телекоммуникации (телекоммуникационные сети, цифровые или аналоговые);
- сети передачи данных (электронные системы и сети передачи данных).

Методика OSSTMM содержит разделы (в целом наблюдается аналогия с ГОСТ Р ИСО/МЭК 27001):

- определение рамок тестирования, ролей и процессов;
- анализ безопасности объекта;
- показатели (метрики) безопасности объекта;
- анализ социальных процессов в персонале объекта тестирования;
- процесс тестирования;
- тестирование устойчивости персонала;
- тестирование безопасности физической инфраструктуры;
- тестирование безопасности беспроводных технологий;
- тестирование безопасности телекоммуникационных технологий;
- тестирование безопасности данных;
- рекомендации по следованию национальным стандартам и соглашениям;
- подготовка отчета о тестировании.

Методика OSSTMM может быть использована как на этапе предварительной оценки защищенности объекта, так и на этапе разработки объекта для проверки функций и мер обеспечения ИБ.

3. Open Web Application Security Project (OWASP)

Методика Open Web Application Security Project (OWASP) создана еще в 20024 г. и развивается в настоящее время международной группой независимых экспертов (сообщество OWASP) [10, 11, 12]. OWASP Web Security Testing Guide v.4.2. на данный момент является актуальной версией, вышедшей в 2020 году[10]. Указанное руководство следует рассма-

8 NIST Special Publications 800-115. Technical Guide to Information Security Testing and Assessment. USA, Gaithersburg, 2008. 80 p. – [Электронный ресурс]. – Режим доступа: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата обращения: 29.06.2022)

9 OSSTMM 3 – The Open Source Security Testing Methodology Manual. – [Электронный ресурс]. – Режим доступа: https://www.isecom.org/OSSTMM.3.pdf (дата обращения: 29.06.2022).

10 OWASP Web Security Testing Guide Version 4.2 – [Электронный ресурс]. – Режим доступа: https://www.owasp.org/index.php/OWASP_Testing_Project (дата обращения: 29.06.2022).

тривать как набор техник (методов), которые можно использовать для поиска уязвимостей в системе безопасности, что особенно важно для типовых удаленных объектов КИИ в отрасли ТЭК. Несмотря на общую ориентацию на тестирование Web-интерфейсов, методика OWASP может быть применена для специальных дополнительных исследований коммуникаций объектов КИИ, в частности, раздел 3 описывает набор тестов, ориентированных на:

- тестирование управления конфигурацией и развертыванием;
- тестировании управления идентификационными данными;
- тестировании аутентификации;
- тестировании авторизации;
- тестировании управления сессиями;
- тестировании «слабой криптографии» (криптографической устойчивости);
- тестировании бизнес-процессов;

Для целей данной публикации важно отметить, что преимущество методики OWASP заключатся в описании тестирования на каждой стадии жизненного цикла объекта.

4. Penetration Testing Execution Standard (PTES)

Стандарт проведения тестирования на проникновение Penetration Testing Execution Standard (PTES) разработан независимыми экспертами, актуальная версия 1.1 от 12 апреля 2022 года[11]. Разделы стандарта представлены основными этапами:

- первоначальное общение (*Pre-engagement Interactions*);
- сбор «разведданных» (анализ открытых источников, анализ «интернет-следа», анализ периметра безопасности, физической инфраструктуры и пр.);
- анализ уязвимостей (ПО, оборудования, VPN, протоколов, интернет-соединений, баз данных и пр.);
- моделирование угроз;
- эксплуатация (атаки на ПО, сетевые протоколы; VPN, DoS-атаки, шлюзы с сетью Интернет и пр.);
- постэксплуатация (формирование программных закладок, получения доступа к важным файлам и авторотационным данным пользователей и пр.);
- отчетность.

Стандарт PTES рекомендуется применять при оценке защищенности объектов на этапе предварительной оценки и на этапе разработки объекта для проверки функций и мер обеспечения ИБ, по аналогии с методикой OSSTMM

5. Information System Security Assessment Framework (ISSAF)

Методика Information System Security Assessment Framework (ISSAF) была разработана группой по безопасности открытых информационных систем (OISSG). Методика ISSAF считается тщательно проработанной методикой, которая может быть адаптирована для оценки ИБ в любой организации [13, 14].

Методика ISSAF по аналогии с представленными выше методиками и стандартами рассматривает несколько «векторов атаки» для объектов КИИ, в том числе:

- определение инфраструктуры объектов КИИ;
- проведение тестов на проникновение для выявления уязвимостей систем;
- нахождение неправильных конфигураций систем и их устранение;
- идентификация и снижение рисков, связанных с ИТ-компонентами, персоналом или бизнес-процессами;
- определение приоритетных мероприятий по оценке в соответствии с критичностью системы и затратами на тестирование;
- обучение персонала (программы осведомленности);
- составление и проверка плана аварийного восстановления;
- анализ проблем безопасности, связанных с аутсорсингом;
- соответствие правовым и нормативным стандартам.

Для целей данной публикации важно, что методика ISSAF включает конкретные виды тестирования на проникновение для объектов КИИ[12], в частности:

- тестирование паролей;
- тестирование безопасности ОС и баз данных;
- тестирование безопасности беспроводных сетей и интернет-коммуникаций;
- тестирование безопасности средств защиты (МЭ, систем обнаружения вторжений, VPN, антивирусных систем и пр.);
- тестирование безопасности пользователей;

11 PTES – The Penetration Testing Execution Standard – [Электронный ресурс]. – Режим доступа: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (дата обращения: 29.06.2022).

12 Тестирование на проникновение, Positive Technologies – [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/services/pentest/(дата обращения: 29.06.2022).

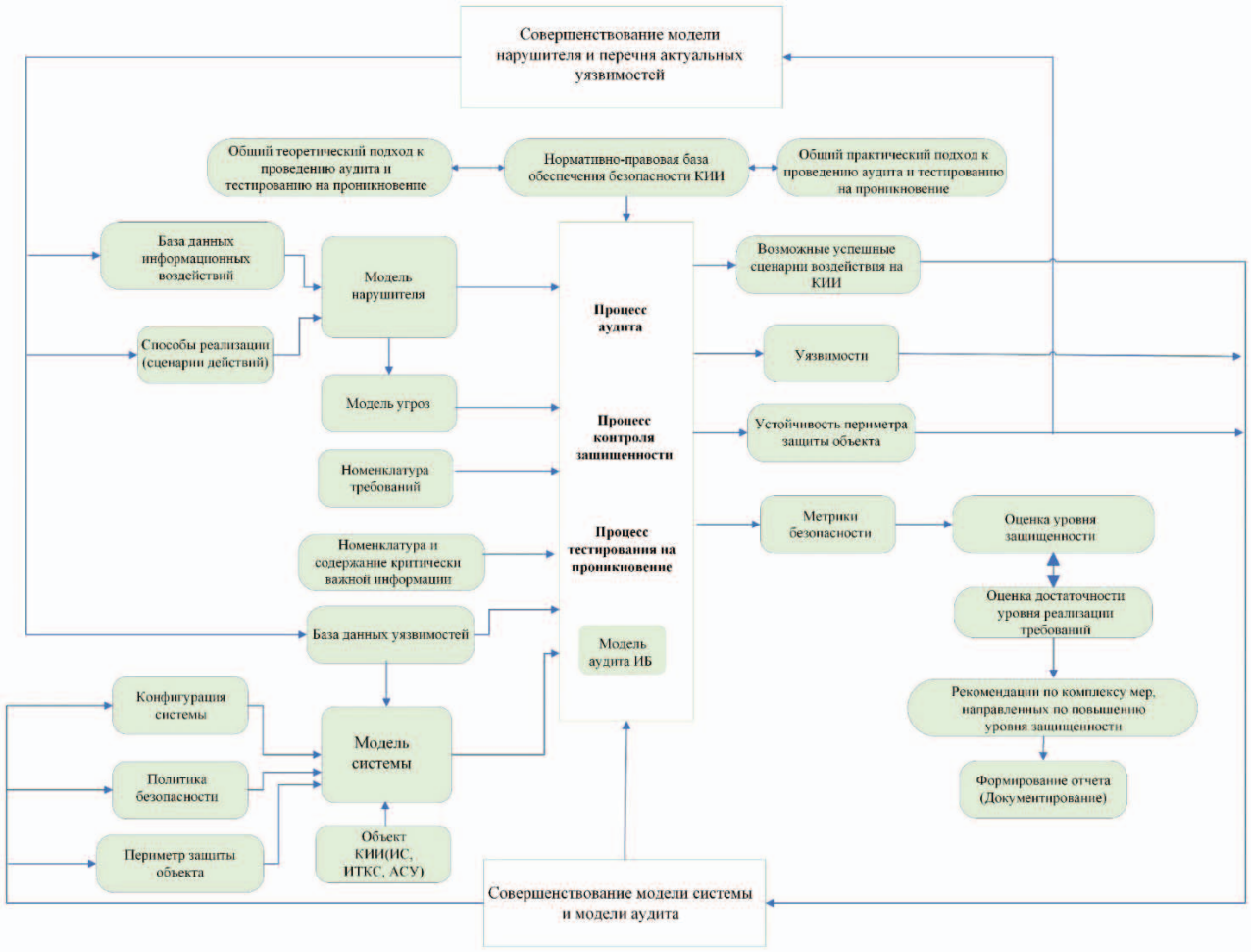

Рис. 6. Модель для контроля защищенности и аудита ИБ для объектов КИИ

— тестирование безопасности исходного кода;
— тестирование социально-психологических аспектов ИБ;
— тестирование физической инфраструктуры.

К недостаткам методика ISSAF можно отнести опциональное требование полного аудита системы и минимальная отчетность в форме устного сообщения о ходе тестирования и критичности выявленных проблем[13]. Методика ISSAF также рекомендуется к применению при оценке защищенности объектов на этапе предварительной оценки и на этапе разработки объекта для проверки функций ИБ, по аналогии с методикой OSSTMM и стандартом PTES. Однако для применения на удаленных объектах ТЭК следует принять заранее риск опциональных требований полного аудита функций безопасности и существующих мер ИБ, что может существенно снизить качество проводимого тестирования.

13 Penetration Testing Methodologies – [Электронный ресурс]. – Режим доступа https://itglobal.com/company/blog/5-pentest-metodologies/ (дата обращения: 29.06.2022).

Часть 3. Модель выполнения контроля защищенности для объектов КИИ

На основании рассмотренных выше существующих методик и стандартов предлагается для выполнения контроля защищенности для объектов КИИ следующая модель (см. рис. 6). Представленная модель обеспечивает два важных преимущества:

— корректность выбора номенклатуры требований исходя из структуры и модели угроз безопасности для объекта КИИ, а также содержания критически важной информации, используемой в процессе функционирования данного объекта;
— объективную оценку достаточности уровня реализации требований к обеспечению безопасности объекта КИИ с учетом его категории.

В рамках предлагаемой методики сформирован перечень мер защиты для объектов КИИ в соответствии с конкретными требованиями ФСТЭК России [16 – 19]. В Таблице 1 приведен фрагмент этих мер применительно к конкретным требованиям контроля

Таблица 1

Меры защиты для объектов КИИ (Фрагмент)

№ п/п	Требования по защите информации	Средства реализации
1	2	3
5	Аудит безопасности	
5.1	АУД.0	Организационные меры
5.2	АУД.1	Средства защиты информации от НСД, сканеры безопасности, средства межсетевого экранирования, организационные меры
5.3	АУД.2	Сканеры безопасности
5.4	АУД.3	Система обеспечения единого времени
5.5	АУД.4	Средства защиты информации от НСД, система обнаружения вторжений, средства межсетевого экранирования, SIEM-системы
5.6	АУД.5	Средства защиты информации от НСД, система обнаружения вторжений, средства межсетевого экранирования
5.7	АУД.6	Система мониторинга, организационные меры
5.8	АУД.7	Средства защиты информации от НСД, сканеры безопасности система обнаружения вторжений, средства межсетевого экранирования, SIEM-системы, организационные меры
5.9	АУД.8	Организационные меры
5.10	АУД.9	Система мониторинга, SIEM-системы
5.11	АУД.10	Организационные меры
5.12	АУД.11	Организационные меры

защищённости – группа аудита безопасности (индекс группы АУД).

Соответственно, выбор, внедрение и периодический анализ корректности настроек применимых мер и средств защиты предлагается выполнять в рамках программы аудитов, запланированной и согласованной со всеми заинтересованными службами для конкретных объектов КИИ. Например, в дополнение к указанным ранее стандартам ГОСТ Р ИСО/МЭК серии 27006 и 27007 в области аудита ИБ, рекомендуется применять специальный «целевой» стандарта ГОСТ Р ИСО/МЭК 27004 как библиотеку метрик ИБ (как показано на рис. 6).

Комбинация рекомендованных мер защиты для объектов КИИ (см. таблицу 1), известных методик риск-менеджмента (стандарты ГОСТ Р ИСО/МЭК серии 31000), а также уникальные свойства объектов КИИ (как показано на рис. 6) позволяют предложить новую модель аудита для объектов КИИ. Определенные предложения в этой области известны, но они касаются описания разрозненных идей в области отдельно применения Байесовых моделей для риск-менеджмента, планирования бизнес-процессов и оценивания рисков и некоторых подходов для гармонизации аспектов ИБ и общей безопасности (safety) применительно к кибер-физическим системам [20 – 22].

Представленная модель также позволяет обеспечить «двойной» режим для полного цикла обеспечения безопасности объектов КИИ – полный национальный режим (на основании только нормативных документов ФСТЭК, формальных моделей угроз, создания моделей нарушителей, применения базы данных угроз ФСТЭК и пр.) и комбинированный режим, который позволяет при необходимости включать «функциональные блоки», заимствованные из лучшего опыта международных научных коллективов (управление рисками, тестирование на проникновение, применение метрик безопасности и пр.). В перспективе представленная модель может включать и новые функциональные расширения, в частности – в области функциональной безопасности (по требованиям ГОСТ Р МЭК серии 61508 / 61511) и определения оценок уровня полноты функциональной безопасности (Safety Integrity level), как новый блок в представленной модели.

Выводы

В представленной публикации рассмотрены кратко основные методики и стандарты, которые могут быть приняты в качестве лучшей практики для контроля

уровня защищенности и аудита ИБ на объектах КИИ. Отмечено, что многие методики (например, методика ISSAF, методика OSSTMM и стандарт PTES) рекомендуются к применению при оценке защищенности объектов на этапах предварительной оценки и разработки объекта для проверки функций, а также существующих мер обеспечения ИБ. В работе отмечено, что целом все рассмотренные методики хорошо взаимоувязаны с известными стандартами – NIST SP 800-115 и ISO/IEC (ГОСТ Р ИСО/МЭК) серии 27000, поскольку общая концепция риск-менеджмента полностью интегрирована во все современные стандарты в области ИБ.

На основе доступных методик предложена новая модель для выполнения контроля защищенности и аудита ИБ для объектов КИИ. Представленная модель обеспечивает два важных преимущества: корректность выбора номенклатуры требований исходя из структуры и модели угроз безопасности для объекта КИИ и объективную оценку достаточности уровня реализации требований к обеспечению безопасности объекта КИИ с учетом его категории. В работе представлен пример реализации требований для обеспечения аудита ИБ для объектов КИИ в соответствии с нормативными документами ФСТЭК для представленной модели.

Научная новизна модели для контроля защищенности и аудита ИБ для объектов КИИ заключается в возможности реализации «двойного» режима для полного цикла обеспечения безопасности объектов КИИ – полного национального режима и комбинированного режима, который позволяет при необходимости включать дополнительные функциональные блоки. Полученные результаты могут быть применены для проектирования, оценки соответствия и модернизации объектов КИИ на объектах ТЭК.

Литература

1. Робертович А.В., Табакаева В.А., Селифанов В. В. Разработка методики аудита кибербезопасности государственных информационных систем, относящихся к значимым объектам критической информационной инфраструктуры, функционирующих на базе центров обработки данных // Интерэкспо Гео-Сибирь. 2020. №1.
2. Нестеровский О.И., Пашковская Е.С., Бутрик Е.Е. Методический подход к организации проведения контроля защищенности информации на объектах критической информационной инфраструктуры // Вестник ВИ МВД России. — 2021. — № 2. — С.126-133.
3. Moudoubah L., Yamami A.E., Mansouri K., Qbadou M. From IT-Service management to IT-Service Governance: An ontological approach for integrated use of ITIL and Cobit Frameworks. International Journal of Electrical and Computer Engineering. 2021. Т. 11. № 6. С. 5292-5300.
4. Moudoubah L., Mansouri K., Qbadou M. Cobit 5 concepts: Towards the development of an ontology model. Lecture Notes in Networks and Systems. 2022. Т. 357 LNNS. С. 247-256.
5. Bernanda D.Y., Angelia M. Evaluation and recommendation IT Governance based on Cobit 5 Framework in Harris Vertu Harmoni Hotel. International Journal of Open Information Technologies. 2021. Т. 9. № 1. С. 86-94.
6. Дорофеев А.В., Лемберская Е.Х., Рауткин Ю.В. Анализ защищенности: нормативная база, методологии и инструменты // Защита информации. Инсайд. 2018. № 4 (82). С. 63-69.
7. Исахин Г.В., Карунас А.Ю. Обзор нормативных документов NIST по безопасности // В сборнике: Сборник избранных статей по материалам научных конференций ГНИИ «Нацразвитие». Международные научные конференции. Санкт-Петербург, 2021. С. 290-292.
8. Choquette S.J., Duewer D.L., Sharpless K.E. NIST Reference Materials: Utility and Future. Annual Review of Analytical Chemistry. 2020. Т. 13. С. 453-474.
9. Eggers S., Le Blanc K. Survey of Cyber risk analysis techniques for use in the Nuclear industry. Progress in Nuclear Energy. 2021. Т. 140. С. 103908.
10. Shahid J., Hameed M.K., Javed I.T., Qureshi K.N., Ali M., Crespi N. A comparative study of Web application security parameters: Current trends and future directions Applied Sciences (Switzerland). 2022. Т. 12. № 8.
11. Rodríguez G.E., Benavides D.E., Torres J.G., Flores P. Cross-site (XSS) attacks and mitigation: A survey. Computer Networks. 2020. Т. 166. С. 106960.
12. Archana Devi R., Amritha C., Sai Gokul K., Ramanuja N., Yaswant L. Prevention and detection of SQL injection using query tokenization. Lecture Notes in Networks and Systems. 2021. Т. 127. С. 165-172.
13. Caturano F., Perrone G., Romano S.P. Hacking Goals: A Goal-centric Attack classification framework. Lecture Notes in Computer Science. 2020. Т. 12543 LNCS. С. 296-301.
14. Sanjaya I.G.A.S., Sasmita G.M.A., Arsa D.M.S. Information technology risk-management using ISO 31000 based on ISSAF framework penetration testing (Case study). International Journal of Computer Network and Information Security. 2020. Т. 12. № 4. С. 30-40.
15. Макаренко С.И., Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. №4.
16. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. Industrial system security assessment study // В сборнике: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021. 2021. С. 161-164
17. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. A study of modern risk managent methods for industrial safety assurance in the fuel and energy industry // В сборнике: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021. 2021. С. 165-167.
18. Лившиц И.И. Менеджмент рисков в области промышленной безопасности в топливно-энергетических компаниях // Стандарты и качество. 2021. № 1. С. 42-48.

19. Лившиц И.И. К вопросу оценивания безопасности промышленных систем управления // Автоматизация в промышленности. 2021. № 7. С. 3-7.
20. Parviainen T., Haapasaari P., Kuikka S., Helle I., Goerlandt F. Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-Art, implementation benefits and challenge, and future research directions. Journal of Environmental Management. 2021. Т. 278. С. 111520.
21. Lukashuk N.A., Hisham H.A. International experience in business planning and risk assessment. Proceeedings of BSTU. Issue 5. Economics and management. 2021. № 1 (244). С. 169-173.
22. ji Z., Yang S.-H., Cao Y., Wang Y., Zhou C., Yue L., Zhang Y. Harmonizing Safety and security risk analysis and prevention in Cyber-Physical systems. Process Safety and Environmental Protection: Transactions of the Institution of Chemical Engineers, Part B. 2021. Т. 148. С. 1279-1291.

RESEARCH OF METHODS FOR MONITORING THE LEVEL OF INFORMATION SECURITY AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

***Livshitz I.I.*[14], *Baksheev A.S.*[15]**

Abstract

Purpose of work *is to analyze the existing practices of performing security analysis and IT-security audit (NIST, OWASP, Cobit, OSSTMM, PTES and GOST R ISO/IEC), used to obtain objective and reliable data for operational security assessments of the CII objects and development of an IT-security audit model for CII objects.*

Research method: *methods of analysis and structural decomposition from the theory of system analysis, identifying signs essential for optimizing the process of IT-security audit for CII objects.*

Research result: *include the detailed analysis and comparison of the existing best practices for performing security analysis and IT-security audit (NIST, OWASP, Cobit, OSSTMM, PTES and GOST R ISO/IEC) for CII objects. A model of IT-security audit for CII objects has been developed.*

Scientific novelty: *an IT-security audit model for CII facilities, characterized by the possibility of a "dual" mode for a full cycle of ensuring the safety of CII facilities – a full national conditional mode and a combined conditional mode, which allows, if necessary, to include additional functional blocks.*

Keywords: *threats, vulnerabilities, standard, risk, audit, controls, information security, NIST, OWASP, Cobit, OSSTMM, PTES, ISSAF.*

References

1. Robertovich A.V., Tabakaeva V.A., Selifanov V. V. Razrabotka metodiki audita kiberbezopasnosti gosudarstvennyh informacionnyh sistem, otnosyashchihsya k znachimym ob"ektam kriticheskoj informacionnoj infrastruktury, funkcioniruyushchih na baze centrov obrabotki dannyh // Interekspo Geo-Sibir'. 2020. №1.
2. Nesterovskij O.I., Pashkovskaya E.S., Butrik E.E. Metodicheskij podhod k organizacii provedeniya kontrolya zashchishchennosti informacii na ob"ektah kriticheskoj informacionnoj infrastruktury // Vestnik VI MVD Rossii. — 2021. — № 2. — S.126-133.
3. Moudoubah L., Yamami A.E., Mansouri K., Qbadou M. From IT-Service management to IT-Service Governance: An ontological approach for integrated use of ITIL and Cobit Frameworks. International Journal of Electrical and Computer Engineering. 2021. Т. 11. № 6. S. 5292-5300.
4. Moudoubah L., Mansouri K., Qbadou M. Cobit 5 concepts: Towards the development of an ontology model. Lecture Notes in Networks and Systems. 2022. Т. 357 LNNS. S. 247-256.
5. Bernanda D.Y., Angelia M. Evaluation and recommendation IT Governance based on Cobit 5 Framework in Harris Vertu Harmoni Hotel. International Journal of Open Information Technologies. 2021. Т. 9. № 1. S. 86-94.
6. Dorofeev A.V., Lemberskaya E.H., Rautkin YU.V. Analiz zashchishchennosti: normativnaya baza, metodologii i instrumenty // Zashchita informacii. Insajd. 2018. № 4 (82). S. 63-69.
7. Isahin G.V., Karunas A.YU. Obzor normativnyh dokumentov NIST po bezopasnosti //V sbornike: Sbornik izbrannyh statej po materialam nauchnyh konferencij GNII "Nacrazvitie". Mezhdunarodnye nauchnye konferencii. Sankt-Peterburg, 2021. S. 290-292.
8. Choquette S.J., Duewer D.L., Sharpless K.E. NIST Reference Materials: Utility and Future. Annual Review of Analytical Chemistry. 2020. Т. 13. S. 453-474.

14 Ilya I. Livshitz, Dr.Sc., Professor, ITMO University, St. Petersburg, Russia. E-mail: Livshitz.il@yandex.ru

15 Andrew S. Baksheev, student, ITMO University, St. Petersburg, Russia. E-mail: Baksheev.Andrey@yandex.com

9. Eggers S., Le Blanc K. Survey of Cyber risk analysis techniques for use in the Nuclear industry. Progress in Nuclear Energy. 2021. T. 140. S. 103908.
10. Shahid J., Hameed M.K., Javed I.T., Qureshi K.N., Ali M., Crespi N. A comparative study of Web application security parameters: Current trends and future directions Applied Sciences (Switzerland). 2022. T. 12. № 8.
11. Rodríguez G.E., Benavides D.E., Torres J.G., Flores P. Cross-site (XSS) attacks and mitigation: A survey. Computer Networks. 2020. T. 166. S. 106960.
12. Archana Devi R., Amritha C., Sai Gokul K., Ramanuja N., Yaswant L. Prevention and detection of SQL injection using query tokenization. Lecture Notes in Networks and Systems. 2021. T. 127. S. 165-172.
13. Caturano F., Perrone G., Romano S.P. Hacking Goals: A Goal-centric Attack classification framework. Lecture Notes in Computer Science. 2020. T. 12543 LNCS. S. 296-301.
14. Sanjaya I.G.A.S., Sasmita G.M.A., Arsa D.M.S. Information technology risk-management using ISO 31000 based on ISSAF framework penetration testing (Case study). International Journal of Computer Network and Information Security. 2020. T. 12. № 4. S. 30-40.
15. Makarenko S.I., Smirnov G.E. Analiz standartov i metodik testirovaniya na proniknovenie // Sistemy upravleniya, svyazi i bezopasnosti. 2020. №4.
16. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. Industrial system security assessment study // V sbornike: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021. 2021. S. 161-164
17. Livshitz I.I., Lontsikh P.A., Lontsikh N.P., Golovina E.Y., Safonova O.M. A study of modern risk managent methods for industrial safety assurance in the fuel and energy industry // V sbornike: Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», T and QM and IS 2021. 2021. S. 165-167.
18. Livshic I.I. Menedzhment riskov v oblasti promyshlennoj bezopasnosti v toplivno-energeticheskih kompaniyah // Standarty i kachestvo. 2021. № 1. S. 42-48.
19. Livshic I.I. K voprosu ocenivaniya bezopasnosti promyshlennyh sistem upravleniya // Avtomatizaciya v promyshlennosti. 2021. № 7. S. 3-7.
20. Parviainen T., Haapasaari P., Kuikka S., Helle I., Goerlandt F. Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-Art, implementation benefits and challenge, and future research directions. Journal of Environmental Management. 2021. T. 278. S. 111520.
21. Lukashuk N.A., Hisham H.A. International experience in business planning and risk assessment. Proceeedings of BSTU. Issue 5. Economics and management. 2021. № 1 (244). S. 169-173.
22. ji Z., Yang S.-H., Cao Y., Wang Y., Zhou C., Yue L., Zhang Y. Harmonizing Safety and security risk analysis and prevention in Cyber-Physical systems. Process Safety and Environmental Protection: Transactions of the Institution of Chemical Engineers, Part B. 2021. T. 148. S. 1279-1291.