РАЗРАБОТКА МЕТОДИКИ КОНТРОЛЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Бакшеев А. С.[1], Лившиц И. И.[2]

Целью работы *является повышение уровня защищенности субъектов критической информационной инфраструктуры (КИИ) за счет использования модели «двойного» режима для реализации гарантированного замкнутого цикла обеспечения безопасности объектов КИИ – полного национального режима и комбинированного режима.*

Метод исследования: *для достижения цели работы применялись методы анализа, сравнения, обобщения, структурной декомпозиции из теории системного анализа, определение критериев для контроля уровня защищенности информации объектов КИИ.*

Результат исследования: *в работе представлен детальный анализ и сопоставление существующих концепций по контролю уровня защищенности информации, применяемых для получения определенного заданного уровня защищенности. Предложена методика контроля уровня защищенности информации объектов КИИ, которая учитывает как существующие, так и перспективные проекты методических документов ФСТЭК России. Полученный результат предоставляет лицам, принимающим решения, численные значения оценок, которые могут быть проверены в процессе независимых аудитов и/или определены расчетными методами на основании объективных и достоверных исходных данных. Формирование объективных оценок позволит существенно повысить уровень защищенности информации, поскольку в процессе независимых аудитов обеспечивается объективность при формировании аудиторской выборки, непредвзятость в процессе доказательства аудиторских решений и прослеживаемости аудиторских выводов.*

Научная новизна *заключается в разработке методики контроля уровня защищенности информации объектов КИИ, основанной на модели аудита информационной безопасности для объектов КИИ, которая в свою очередь, базируется на возможности реализации модели «двойного режима» для полного замкнутого цикла обеспечения безопасности объектов КИИ – полный национальный и комбинированный режимы, позволяющие при необходимости включать дополнительные функциональные блоки.*

Ключевые слова: *меры защиты, уязвимости, стандарт, риск, остаточный риск, аудит, информационная безопасность, тестирование на проникновение, принцип Парето, доминирование.*

DOI:10.21681/2311-3456-2023-2-85-98

Введение

На данный момент в РФ определены следующие основные направления обеспечения информационной безопасности (ОИБ), исходя из Доктрины информационной безопасности РФ[3] и Стратегии национальной безопасности Российской Федерации (утвержденна Указом Президента Российской Федерации от 2 июля 2021 г. № 400)[4]:

— повышение защищенности и устойчивости функционирования объектов критической информационной инфраструктуры (КИИ), развитие меха-

3 Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646) // Официальный интернет-портал правовой информации.

4 Стратегия национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 2 июля 2021 г. № 400) // Официальный интернет-портал правовой информации

1 Бакшеев Андрей Сергеевич, магистрант группы N42532c Университета ИТМО, Санкт-Петербург, Россия. E-mail: andrei.baksheev@gmail.com

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

низмов обнаружения и предупреждения угроз и ликвидации последствий их проявления;
- развитие отрасли ИТ, а также совершенствование деятельности по разработке, производству и эксплуатации средств защиты информации (СЗИ);
- снижение до минимально возможного уровня утечек информации ограниченного доступа и персональных данных (ПДн);
- развитие кадрового потенциала в области ОИБ.

Существующие реалии и текущая ситуация в РФ во многом изменили требования к контролю уровня защищенности информации и к обеспечению ИБ в целом – Указ № 166[5] и Указ № 250[6]. Регуляторами было подготовлено более 50 рекомендаций по повышению защищенности информационной инфраструктуры и решению задач ОИБ. Выделим наиболее важные из них:
- меры по повышению защищенности официальных сайтов органов государственной власти и организаций;
- меры по предотвращению несанкционированного распространения уволенными администраторами систем защищаемой информации;
- меры по предотвращению реализации угроз безопасности информации (УБИ), связанных с утечкой защищаемой информации;
- меры по предотвращению реализации УБИ, связанных с внедрением вирусов шифровальщиков;
- меры по предотвращению реализации УБИ, связанных с фишингом;
- меры по предотвращению реализации УБИ, направленных на отказ в обслуживании;
- меры по обновлению применяемого в информационных системах (ИС) иностранных компонент;
- меры по повышению защищенности информационной инфраструктуры РФ;
- рекомендации по повышению защищенности информационной инфраструктуры РФ, содержащие дополнительные меры ИБ, направленные на противодействие компьютерным атакам на информационную инфраструктуру РФ.

Обеспечение безопасности объектов КИИ является важной проблемой в настоящее время. Это обусловлено растущей зависимостью общества от данных систем, а также УБИ, таких как кибератаки на инфраструктуру, стихийные бедствия и др. Последствия, которые приводят к нарушению функционирования таких объектов, могут привести к серьезным потерям, начиная от финансовых и заканчивая нарушением работы основных служб электроэнергетики, топливно-энергетического комплекса, оборонной промышленности, медицины, связи и транспорта. Поэтому важность использования эффективных методов контроля защищенности для минимизации рисков инцидентов ИБ и обеспечения надежности и нормального функционирования объектов КИИ предполагает в целом использование полного национального подхода. Данный подход определенно должен быть комплексным и включать оценку рисков (остаточных рисков), регулярный мониторинг и тестирование ИС, планирование реагирования на инциденты, соблюдение стандартов, постоянное улучшение защиты объектов КИИ. Субъекты КИИ должны быть осведомлены о последствиях актуальных УБИ, используемых ИТ, передовых практиках ИБ и пр. для того, чтобы эффективно защищать свои системы. Объекты КИИ важны для экономической стабильности, национальной безопасности, здоровья и благополучия населения. Использование методов контроля может быть оптимизировано для обеспечения как максимально высокого (возможного), так и приемлемого (заданного) уровня защиты (как от внутренних, так и внешних УБИ), обеспечивая доступность, конфиденциальность и целостность.

Актуальность исследования заключается в разработке методики контроля уровня защищенности информации объектов КИИ, основанной на использовании методик аудита ИБ, предложенной модели для контроля защищенности и аудита ИБ для объектов КИИ, и тестирования на проникновение (ТнП) в рамках общего цикла обеспечения ИБ.

Объектом исследования является контроль уровня защищенности информации объектов КИИ.

Предметом исследования является методика контроля уровня защищенности информации объектов КИИ.

5 Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»// Официальный интернет-портал правовой информации

6 Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»//Официальный интернет-портал правовой информации. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

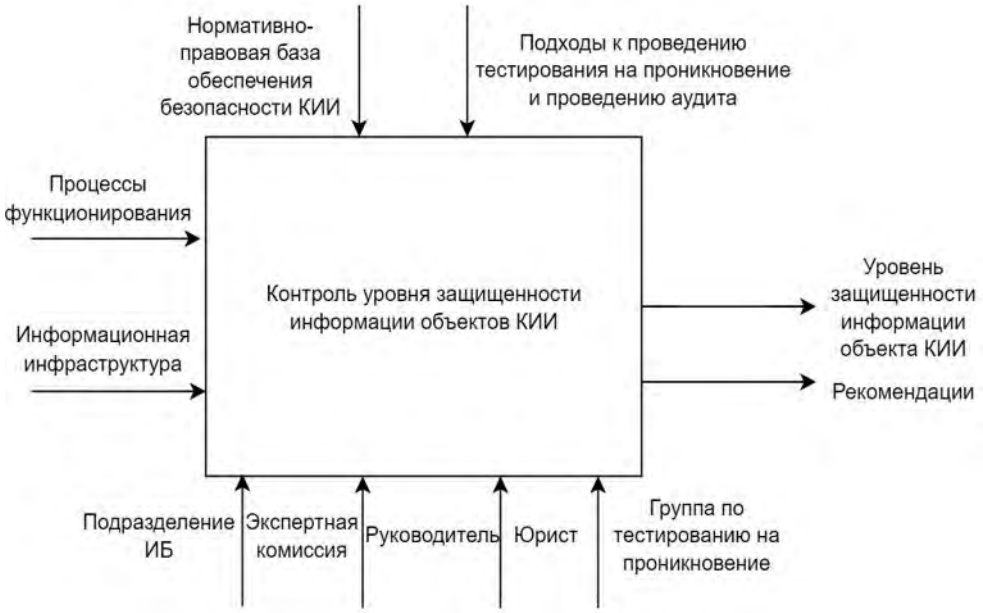

Рис.1. Диаграмма A0 в нотации IDEF0 (Контроль уровня защищенности информации)

Вербальная постановка задачи

Дано: известные практики и проекты методик ФСТЭК России (Приказ № 239[7]), направленные на выполнение анализа (контроля) защищенности и аудита ИБ, национальные стандарты ГОСТ Р ИСО/МЭК, а также доступные международные и федеральный стандарты и методики (NIST[8], COBIT, OWASP, OSSTMM, Garther[9], PTES[10]), а также модель аудита ИБ, которая использует «двойной» режим (полный национальный и комбинированный режимы);

Необходимо: на основе проведенного анализа известных практик анализа защищенности и предложенной модели аудита ИБ, которая использует «двойной» режим и обладает оптимальными характеристиками для соответствия требованиям обеспечения безопасности объектов КИИ, разработать методику контроля уровня защищенности информации объектов КИИ.

Исходные данные: требования для обеспечения безопасности объектов КИИ в Российской Федерации, проекты методик ФСТЭК России, предложенная модель аудита ИБ.

Ограничения: состав мер защиты для объектов КИИ, определенный регулятором ФСТЭК России, известные ограничения процессов аудита ИБ и ТнП, функциональные ограничения компонентов и типов объектов КИИ, ограничения временных и стоимостных ресурсов для выполнения контроля уровня защищенности информации и ТнП.

Задачи исследования определены следующим образом:

- построение модели проведения контроля уровня защищенности информации объектов КИИ в нотации IDEF0 и определение порядка выполнения контроля уровня защищенности информации объектов КИИ с использованием «двойного» режима;
- определение ПО для ТнП в рамках предлагаемой методики;
- сравнение существующих методик по контролю уровня защищенности информации в соответствии с критериями (сопоставление);
- расчет общего уровня защищенности информации объектов КИИ;
- математическое обоснование методики контроля уровня защищенности информации объектов КИИ.

7 Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» // СПС КонсультантПлюс (дата обращения: 28.12.2022).

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: 28.12.2022).

9 Innovation Insight for Attack Surface Management // Gartner, Inc. — 2022.

10 Implement a Continuous Threat Exposure Management(CTEM) Program // Gartner, Inc. — 2022.

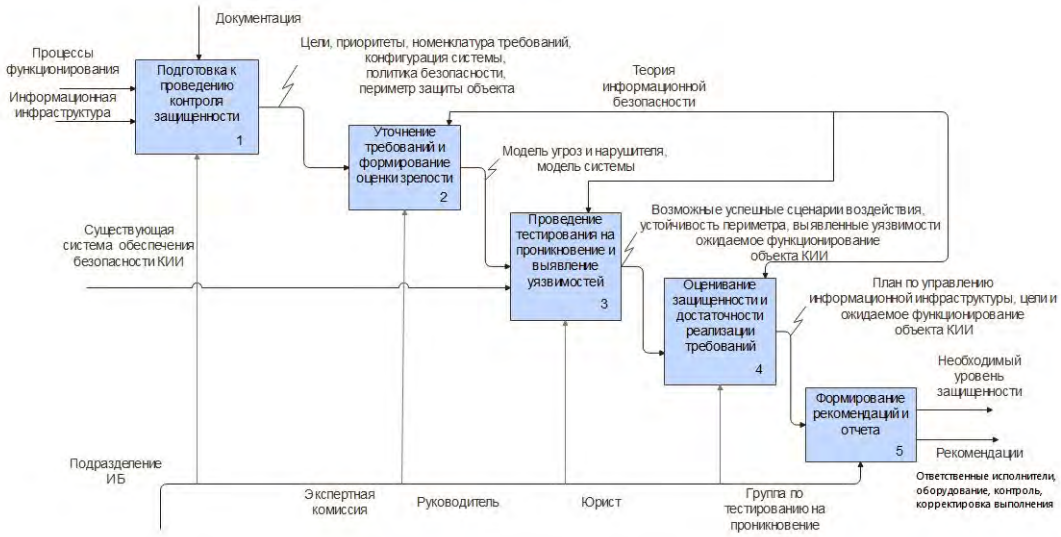

Рис.2. Диаграмма А1. Порядок действий при контроле уровня защищенности информации объектов КИИ в нотации IDEF0

Защитные меры		Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5	Средства реализации	Значение текущего уровня	Рекомендуемый уровень	Общий текущий уровень	Общий рекомендуемый уровень
ИАФ	Идентификация и аутентификация	Базовая идентификация и аутентификация собственных пользователей	Многофакторная аутентификация собственных пользователей	Идентификация и аутентификация устройств	Идентификация и аутентификация внешних пользователей	Федеративная система идентификации и аутентификации при доступе к внутренним и внешним ресурсам	Организационные меры, средства защиты информации от НСД, встроенные механизмы защиты ОС, система управления доступом (IDM), системы мониторинга,средства межсетевого экранирования, межсетевой экран,DLP-система,система криптографической защиты информации	2	4	3	4
УПД	Управление доступом	Базовое управление доступом пользователей	Реализация и контроль принципа минимума привилегий. Управление доступом устройств	Реализация защищенного удаленного и мобильного доступа пользователей и устройств	Контроль доступа из внешних систем, а также в облачных средах	Управление атрибутами безопасности и сквозной политикой управления доступом пользователей и устройств во внутренней сети, на периметре, в облаках и на мобильных устройствах	Организационные меры, средства защиты информации от НСД, встроенные механизмы защиты ОС, средства межсетевого экранирования, межсетевой экран,модуль доверенной загрузки, система криптографической защиты информации	3	5		

Рис.3. Часть защитных мер и нахождение общего уровня зрелости

Методика контроля уровня защищенности информации объектов КИИ

Текущая модель для решения поставленной задачи – контроля защищенности и аудита ИБ для объектов КИИ, позволяет обеспечить реализацию модели «двойного» режима для полного замкнутого цикла обеспечения безопасности объектов КИИ [1]:

- полный национальный режим (на основании только нормативных документов ФСТЭК России, формальных моделей УБИ, создания моделей нарушителей, применения БДУ ФСТЭК России и пр.)
- комбинированный режим, который позволяет при необходимости включать «функциональные блоки», заимствованные из лучшего опыта международных научных коллективов (управление рисками (остаточными рисками), ТнП, применение численных метрик безопасности и пр.) [2,3,4].

В рамках работы представлена обобщенная модель в нотации IDEF0 (рис.1)

Процесс контроля уровня защищенности информации объектов КИИ (рис. 1) определяет процессы функционирования и информационную инфраструктуру, которые имеют значительную ценность для субъекта КИИ и государства [5,6]. Возможность проведения контроля уровня защищенности информации определяется исходя из норм применимого законодательства и нормативных документов регуляторов (ФСТЭК России) по обеспечению безопасности объектов КИИ, методик ТнП.

Для решения поставленной задачи предлагается следующий порядок выполнения контроля уровня защищенности информации объектов КИИ с использованием модели «двойного» режима (рис. 2):

- подготовка к проведению контроля защищенности;
- уточнение требований и формирование оценки зрелости;
- проведение ТнП и выявление уязвимостей;
- оценивание защищенности и достаточности реализации требований;

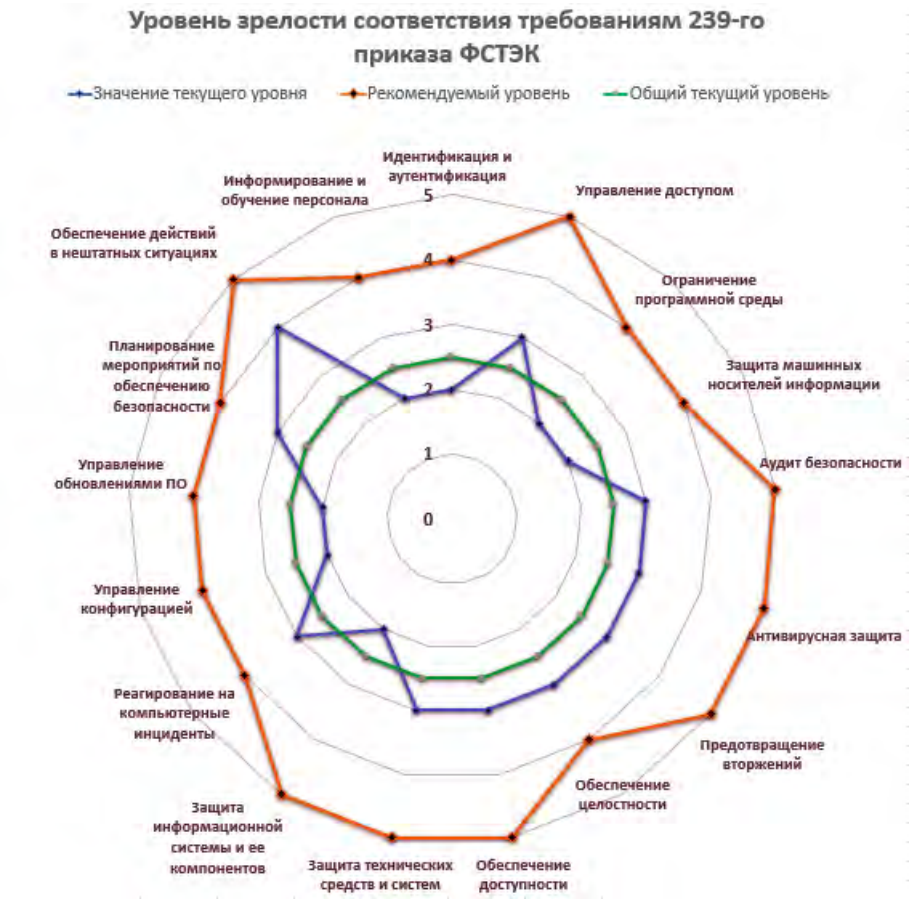

Рис.4. Лепестковая диаграмма «Уровня зрелости защитных мер»

— формирование рекомендаций и отчета.

В рамках оценки зрелости требований используется концепция, предложенная специалистами ИБ[11]. Оценка реализации защитных мер строится на пяти уровнях зрелости, каждый из которых характеризует применение тех или иных технологий или используемого уровня автоматизации. Данное решение было дополнено СЗИ и расчетом общего уровня зрелости защитных мер в соответствии с нормативными документами ФСТЭК России (рис.3). Данный расчет является связующей частью в национальном режиме для нахождения общего уровня защищенности информации в методике контроля уровня защищенности информации объектов КИИ.

В качестве визуализации уровня зрелости защитных мер используется вариант лепестковой диаграммы (рис.4). Визуализация в виде лепестковой диаграммы представляет наглядное сопоставление численных значений текущего и рекомендуемого уровней зрелости защитных мер. Примем во внимание, что общая категория «защитные меры» может быть дополнительно специфицирована, например – СЗИ и средства криптографической защиты информации (СКЗИ).

В мировой практике общий порядок контроля уровня защищенности может включать различные этапы, которые в предложенном методе «двойного» режима могут дополняться как функциональные блоки методики для контроля защищенности и аудита ИБ для объектов КИИ, и общая оценка будет оцениваться в зависимости от отдельных уровней оценки [7 – 11]. Выделим основные этапы общего порядка выполнения аудита ИБ, которые реализуются в предложенной методике для целей контроля уровня защищенности информации объектов КИИ:

1. Подготовка:
   — Определение области контроля и объектов, подлежащих проверке;
   — Сбор группы экспертов;
   — Определение критериев и методов оценки уровня контроля;
   — Разработка графика проведения контроля;
2. Сбор информации об объекте:

11 Калькулятор оценки технологической зрелости соответствия 239-му приказу. – [Электронный ресурс]. – Режим доступа: https://lukatsky.ru/legislation/239.html (дата обращения: 28.12.2022).

— Получение информации о проверяемом объекте и его системе защиты;
— Изучение документации для объекта;

3. Оценка уровня безопасности:
— Оценка соответствия системы ИБ объекта действующему законодательству и нормативным актам;
— Оценка адекватности мер безопасности и степени их реализации;
— Выявление уязвимостей и УБИ объекта;

4. Подготовка промежуточного отчета:
— Обобщение результатов оценки и формирование рекомендаций по повышению уровня безопасности объекта;
— Предоставление подробного описания процесса оценки и используемых методов;
— Представление отчета ответственным органам и доступ для соответствующих сторон.

5. Мониторинг и проведение мероприятий по защите:
— Мониторинг выполнения рекомендаций;
— Проведение проверок для определения надежности и функционирования объекта;
— Обновление системы защиты на основе результатов контроля и изменения текущих угроз;

6. Тестирование на проникновение:
— Проведение ТнП для проверки уровня защищенности объекта и выявления любых слабых мест;
— Использование различных инструментов для ТнП, инструментов поиска уязвимостей и сетевого анализа;

7. Анализ поведения пользователей:
— Анализ поведения пользователей и их соответствие политикам и процедурам ИБ;
— Оценка эффективности программ повышения осведомленности и обучения пользователей в области ИБ;

8. Оценка физической безопасности:
— Оценка мер физической безопасности, применяемых для защиты объекта;
— Оценка мер по защите от несанкционированного доступа;

9. Оценка рисков (остаточных рисков):
— Выполнение оценки рисков для выявления потенциальных угроз и уязвимостей ИБ объекта;
— Оценка потенциального воздействия каждого риска и расстановка приоритетов в зависимости от их вероятности и последствий;
— Оценка остаточных рисков

10. Реагирование на инциденты:
— Разработка и внедрение плана реагирования на инциденты;
— Определение, что в план реагирования на инциденты включены роли и обязанности, процедуры устранения и сдерживания инцидентов, смягчения последствий инцидентов, отчетность и документирование инцидентов;

11. Соответствие требованиям ИБ:
— Соответствие законам и стандартам ИБ;
— Регулярная оценка и подтверждение соответствия требованиям с помощью внутренних и внешних аудитов.

12. Заключение и рекомендации:
— Предоставление окончательного заключения об уровне безопасности информационной системы объекта;
— Выработка конкретных рекомендаций по повышению уровня безопасности и снижению выявленных рисков (остаточных рисков);

13. Непрерывное совершенствование:
— Оценка применяемых средств контроля и выстроенных процессов обеспечения безопасности;
— Поддержание приемлемого уровня защиты систем;
— Внесение улучшений по мере необходимости.

Само ТнП, предложенное как функциональный блок модели, может применяться на объектах КИИ как дополнительный независимый способ контроля уровня защищенности информации объектов КИИ. Определим далее основные шаги проведения ТнП:

1. Планирование и подготовка:
— Определение области тестирования;
— Получение одобрения и разрешения от соответствующих заинтересованных сторон;
— Сбор команды экспертов;
— Разработка графика и плана тестирования;

2. Сбор информации:
— Сбор информации о целевой системе и используемых мерах обеспечения безопасности;
— Определение потенциальных векторов атак и точек входа в целевую ИС;

3. Поиск уязвимостей:
— Использование инструментов для выявления потенциальных уязвимостей в ИС;
— Оценка результатов проверки и определение приоритетных уязвимостей для тестирования;

4. Тестирование и эксплуатация уязвимостей:
— Проведение ручных и автоматических тестов на проникновение для попытки использования уязвимостей;

Таблица 1

Программные средства, используемые для ТнП

№ п/п	Тип ПО	Перечни ПО
1	Использование открытых источников (OSINT)	Maltego, Sherlock, Maigret, Snoop, sherlock-go, Investigo, Metagoofil, Foca
2	ТнП	Driftnet, Dsniff, Ethereal, Ettercap, Kismet, Nessus, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer, Wireshark, Netcat, Ngrep, TCPdump
3	Анализ сети	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Netcat, Nmap, P0f, Tctrace, Umit, Cryptcat, Firewalk
4	«Снифферы» и программы захвата трафика	Dsniff, Ettercap, Ethereal, Kismet, Filesnarf, Mailsnarf, Msgsnarf, Ntop, Ngrep, TCPdump, Phoss, SinFP, SMB Sniffer, Wireshark, Webspy
5	Идентификация портов и сетевых сервисов	Amap, AutoScan, Netdiscover, Netcat, Nmap, P0f, Umit, UnicornScan
6	Сканирование уязвимостей	Commix, Exodus, Firewalk, GFI LANguard, Hydra, Metasploit, Nessus, Nmap, Paros Proxy, Snort, SuperScan
7	Сканирование беспроводных сетей	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI, GPSdrive, LANguard, Kismet, MACchanger, WifiTAP
8	Проверка целостности файлов	Autopsy, Biew, Bsed, Coreography, Foremost, Hashdig, Rifiuti, RootkitHunter, Sleuthkit
9	Взлом паролей	Allwords2, chntpw, Cisilia, Djohn, Hydra, Mimikatz, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack, WebCrack
10	Тестирование удаленного доступа	Apache Server, IKEProbe, IKE-Scan, Net-SNMP, SSHD, TFTPD, PSK-Crack, VNC_bypauth, VNC Server
11	Тестирование безопасности приложений	Acunetix, CIRT Fuzzer, Fortify WebInspect, Fuzzer 1.2, NetSed, PT Application Inspector, Paros Proxy, Peach, Synopsys Managed DAST

— Имитирование реальных атак и оценка эффективности мер обеспечения безопасности;

5. Отчетность:

— Предоставление подробного отчета о результатах тестирования;

— Определение обнаруженных уязвимостей и их влияние, которое они могут оказать на безопасность целевой системы;

— Выработка рекомендации по повышению безопасности целевой ИС.

ТнП является важным компонентом определения защищенности информации целевой системы и применяемых СЗИ (СКЗИ), поскольку оно обеспечивает практическую, объективную и непредвзятую оценку безопасности исследуемой системы. Данный функциональный блок в предложенной методике позволяет выявлять и устранять слабые места в системе защиты, прежде чем они могут быть использованы злоумышленниками.

Используемое ПО для тестирования на проникновение в рамках методики

В рамках проведения тестирования объекта могут использоваться следующие программные средства (табл.1). В отличие от исходной разрозненной информации, перечни, предложенные в [12,13], обобщены. Часть предложенных программных средств используется для реализации способов ТнП из комплекса BackTrack и Knoppix STD.

Сравнение существующих методик по контролю уровня защищенности информации

На данный момент ФСТЭК России предложены следующие проекты методик: «Методика оценки (анализа) защищенности информационных систем»

и «Методика оценки состояния защиты информации (обеспечения безопасности) в органе (организации)». Рассмотрим их более подробно далее.

1. Проект «Методики оценки (анализа) защищенности информационных систем»

Проект «Методики оценки (анализа) защищенности информационных систем» определяет порядок проведения работ по оценке (анализу) защищенности конкретно для ИС в порядке:

- определение целей проведения контроля (анализа) защищенности;
- определение области проведения контроля (анализа) защищенности в ИС;
- выполнение работ по контролю (анализу) защищенности;
- оформление результатов контроля (анализа) защищенности.

Конкретно работы по оценке (анализу) защищенности включают:

- сбор информации об ИС;
- анализ уязвимостей ИС, включая анализ уязвимостей инфраструктуры, периметра, приложений, беспроводных сетей;
- тестирование ИС, включая тестирование периметра, внутренней инфраструктуры, беспроводных сетей, социотехническое тестирование.

2. Проект «Методики оценки состояния защиты информации (обеспечения безопасности)

Проект «Методики оценки состояния защиты информации (обеспечения безопасности) в органе (организации)» опубликован на уровне концепция модели. Определены уровни защищенности, показатели, частные показатели для организации и управления защитой (А), внедрение мер защиты информации (Р), поддержка уровня защиты информации (Q) Меры защиты, предложенные в проекте методике, описывают общее состояние ИБ организации, не затрагивая аспекты поиска конкретно слабых мест в системе защиты и не затрагивают, к сожалению, оценивание рисков (рис.5).

В рамках разработки методики контроля уровня защищённости информации объектов КИИ предложена составная концепция Garther – «exposure management». Данная концепция позволяет оценивать незащищенность информационной инфраструктуры, что позволяет построить обобщенную методику, которая будет учитывать законодательную базу, номенклатуру требований, оценивание примененных СЗИ (СКЗИ), проведение ТнП, выпуск рекомендаций. Отметим, что EASM и CAASM – архитектурные платформы, которые используются для управления ИБ. EASM представляет общую структуру и методологию по управлению безопасностью и охватывает все аспекты безопасности, включает как физическую безопасность объекта, сетевую, инвентаризацию активов, управление уязвимостями. CAASM фокусируется на определении, защите и управлении критически важными активами, включает разработку политик и процедур безопасности, обучение и поддержку сотрудников, постоянный мониторинг и оценку безопасности [12,13]. Основные характеристики «Exposure management» Gartner представлены в табл.2.

Рис.5. Проект Методики оценки состояния защиты информации (обеспечения безопасности) в органе (организации)

Таблица 2

«Exposure management» Gartner

Цель	Деятельность	Сфера применения	Поддерживающие платформы
Инвентаризация активов	Проверка и подсчет	— внешний периметр – приложение; — сканирование — расстановка приоритетов	— управление поверхностью внешней атаки (EASM); — управление поверхностью атаки киберактивов (CAASM); — защита от цифровых рисков; — оценка уязвимостей
Управление уязвимостями	Оценка уязвимостей	— внешний периметр – приложение; — сканирование — остановка, как только «найдено»	— управление поверхностью внешней атаки (EASM); — оценка уязвимости (VA); — технология приоритизации уязвимостей (VPT); — инструментарий для ТнП
Осуществимость атаки	Красная команда «Red team», тестирование системы контроля безопасности	— вектор угрозы; — путь атаки; — назначенная цель	— симулятор атак (BAS) – взлом и закрепление — услуги красной команды (Red team).
Оценка состояния безопасности	Оценка рисков, тренинги центра мониторинга ИБ (SOC)	— Фреймворк тактик, техник и процедур (MITRE TTPs) — контроль безопасности — процесс — люди	— симулятор атак (BAS) – взлом и закрепление; — платформы для проведения киберучений; — управление состоянием безопасности в облаке (CSPM); — управление состоянием безопасности (SSPM)

Сравнение предложенной авторами новой методики и двух проектов ФСТЭК России представлено в табл.3. Критерии сравнения были выбраны исходя из общего анализа существующей на данный момент открытой информации и включают основные характеристики и процессы, которые должны выполняться при ОИБ объектов КИИ. Исходя из результатов сравнения предложенные проекты методик ФСТЭК России охватывают определенные аспекты их использования в конкретной специфике выполнения задач.

Концепция общего уровня защищенности информации объектов КИИ

Для нахождения общего уровня защищенности информации в предложенной авторами новой методике контроля уровня защищенности информации объектов КИИ введем следующие обозначения:

М – общий уровень зрелости защитных мер в соответствии с требованиями регуляторов;

Т – уровень защищенности от внешних воздействий на целевую систему и ТнП;

К – общий уровень защищенности информации объектов КИИ.

Концепция расчета заключается в получении общего уровня защищенности через (1):

$$K = \{M \times T\} \quad (1)$$

где: М – Уровень зрелости, Т – Уровень защищенности.

Предложенные следующие граничные условия:

— М имеет следующие числовые уровни – {1, 2, 3, 4, 5};

— Т имеет следующие числовые уровни – {1, 2, 3};

— К соответствуют {1низкий, 2 средний, 3 высокий };

При нахождении К принимаются следующие численные показатели уровня защищенности:

— Низкий – от 1 до 5;

— Средний – от 6 до 9;

— Высокий – от 10 до 15.

При использовании в новой методике, предложенной авторами, дополнительных функциональных блоков в модели «двойного режима», показатели будут увеличиваться пропорционально начальным значениям, например, через дополнительные коэффициенты.

Уровень М определяется в рамках оценки зрелости, заданной по требованиям регулятора.

Уровень Т определяется в зависимости от проведенных способов закрепления в целевой системе и успеха в использовании эксплуатации уязвимостей. Ему соответствуют:

— {1 – низкий} – число успехов и использование уязвимостей от 9 и больше;
— {2 – средний} – число успехов и использование уязвимостей от 4 до 8;
— {3 – высокий} – число успехов и использование уязвимостей от 1 до 3.

Таблица 3

Сравнение методик

Критерии	Проект «Методика оценки (анализа) защищенности информационных систем»	Проект методики оценки состояния защиты информации (обеспечения безопасности) в органе (организации)	Методика контроля уровня защищенности информации объектов КИИ
Предложено	ФСТЭК России	ФСТЭК России	Авторы
Уровни защищённости	неизвестно	4 уровня (высокий, базовый повышенный, базовый, низкий)	3 уровня (высокий, средний, низкий)
Показатели	неизвестно	(А) Организация и управление защитой информации (Р) Внедрение мер защиты информации (Q) Поддержка уровня защиты информации	(М) – Меры защиты Приказов ФСТЭК, соответствующие одной из категории значимости (О) – Организационно-управленческий аспект защиты (Т) – Проведение ТнП (R) – Поддержка рекомендуемого уровня защиты информации объекта КИИ
Оценка мер защиты	неизвестно	+	+
Оценка рисков	неизвестно	неизвестно	+
Сценарии воздействия на систему	неизвестно	неизвестно	+
Аудит ИБ	неизвестно	внутренний, внешний	внутренний, внешний
Определение периметра защиты	+	+	+
Комбинация «функциональных» блоков (расширение модели методики)	неизвестно	неизвестно	+
Рекомендации по комплексу мер, направленных на повышение уровня защищенности (Отчетность)	неизвестно	–	+
Определены программные средства	неизвестно	неизвестно	В рамках тестирования представлен перечень
Простота использования	+/-	+/-	+/-
Последовательность в реализации и соблюдении политик и процедур ИБ	+	+	+

Математическое обоснование методики контроля уровня защищенности информации

Для сопоставления различных методик (двух проектов методик ФСТЭК России и предложенной авторами методики) используется Принцип Парето. «Оптимальность по Парето», кратко, заключается в следующем: состояние системы, при котором ни один из оцениваемых показателей не может быть улучшен без ухудшения другого показателя [14 – 17].

С точки зрения контроля уровня защищенности информации, оптимальность по Парето может быть применена для оценки компромиссов между затратами и выгодами различных мер безопасности. Например, более масштабное внедрение мер безопасности (СЗИ и/или СКЗИ) может повысить уровень защиты, но также увеличить стоимость эксплуатации. Оптимальным решением будет то, которое обеспечивает заданный приемлемый уровень безопасности при обоснованных наименьших затратах. Оптимальность по Парето может быть использована для определения оптимального баланса между безопасностью и экономической эффективностью в данной ситуации.

Определим набор числовых функций $f_1, f_2 \ldots f_m$, $m \geq 2$, определенных на множестве возможных решений X как критерии оптимальности (целевые функции). Вектор $f = (f_1, f_2, \ldots, f_m)$ называют векторным критерием, который принимает значения в m-мерном пространстве R^m – пространство оценок. Векторная оценка возможного решения $x \in X$ для векторного критерия f определяется по (2):

$$f(x) = (f_1(x), f_2(x), \ldots f_m(x)) \in R^m \quad (2)$$

Все возможные векторные оценки образуют множество возможных оценок (3):

$$Y = f(x) = \{y \in R^m \mid y = f(x) \text{ при } x \in X\} \quad (3)$$

Все возможные выбираемые оценки образуют множество выбираемых векторов (оценок) (4):

$$C(Y) = f(C(X)) = \{y \in Y \mid y = f(x) \text{ при } x \in C(X)\} \quad (4)$$

Многокритериальной задачей (задача многокритериальной оптимизации – МКО) называют задачу выбора, которая включает множество допустимых значений X и векторный критерий f, либо задача МКО состоит в отыскании множества выбираемых решений C(X), таких что $C(X) \subset X$ с учетом отношения предпочтения $\succ_x$ на основе заданного векторного критерия *f*, установленного в соответствии с целями (предпочтениями) лица, принимающего решения (ЛПР). Известно, что решение $x^* \in X$ называют оптимальным по Парето (или парето-оптимальным), если не существует такого возможного решения $x \in X$, для которого выполняется неравенство $f(x) \geq f(x^*)$. Парето-оптимальные решения образуют множество Парето P j (X) по (5):

$$P_j(X) = \{x^* \in X \mid \text{не существует такого } x^* \in X, \text{ для которого } f(x) \geq f(x^*)\}. \quad (5)$$

Принцип Эджвота-Парето гласит, что если ЛПР ведет себя «разумно», то выбираемые решения обязательно должны быть парето-оптимальными [17]. Можно определить «разумность» поведения ЛПР при следующих условиях:

выполнение аксиомы исключения доминирующих векторов: для любой пары допустимых векторов y^1, $y^2 \in Y$, для которых выполнятся $y^1 \succ_y y^2$, выполнено $y^2 \notin C(Y)$;

выполнение аксиомы Парето: для всех пар допустимых решений $x^1, x^2 \in X$, для которых выполнятся неравенство $f(x^1) \geq f(x^2)$, выполняется $x^1 \succ_x x^2$

В практическом аспекте для решения поставленной задачи важно принять к рассмотрению важное свойство множества Парето – существования непустого множества парето-оптимальных векторов. Это означает, например, что при известных критериях *f* (например, бюджет, цели, сроки, персонал), есть принципиальная возможность выбора, например, оптимального набора мер (СЗИ, СКЗИ) для контроля уровня защищенности информации при реализации методики, предложенной авторами. Конкретно, для целей формирования уровня защищенности информации объекта КИИ и рекомендаций – оценивание защищенности, номенклатуры требований, ТнП, могут быть предложены следующие критерии:

f_1 – стоимость проекта контроля защищенности.

f_2 – стоимость ТнП для контроля защищенности.

f_3 – длительность проекта контроля защищенности.

f_4 – объем документации, требуемой для контроля защищенности.

f_5 – стоимость новых контрактов по оказанию услуг после контроля защищенности.

f_6 – стоимость признания выполненных работ по контролю защищенности.

f_7 – доступность национальных экспертов для выполнения контроля защищенности.

f_8 – доступность специалистов для выполнения ТнП.

В рассматриваемом примере оптимизации по Парето имеем:

— 3 варианта $Y = \{y^{(1)}, y^{(2)}, y^{(3)}\}$;

— 8 критериев ($m = 8$);

— Количественную (балльную) шкалу – 5 баллов;

Кроме того, нужно минимизировать ряд критериев:

Таблица 4

Оценка по Парето различных вариантов для оценки защищенности объектов КИИ

Вектор оценок	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
$y^{(1)}$	2	2	1	1	2	2	3	2
$y^{(2)}$	2	3	2	1	3	4	3	3
$y^{(3)}$	3	4	2	2	4	4	5	4

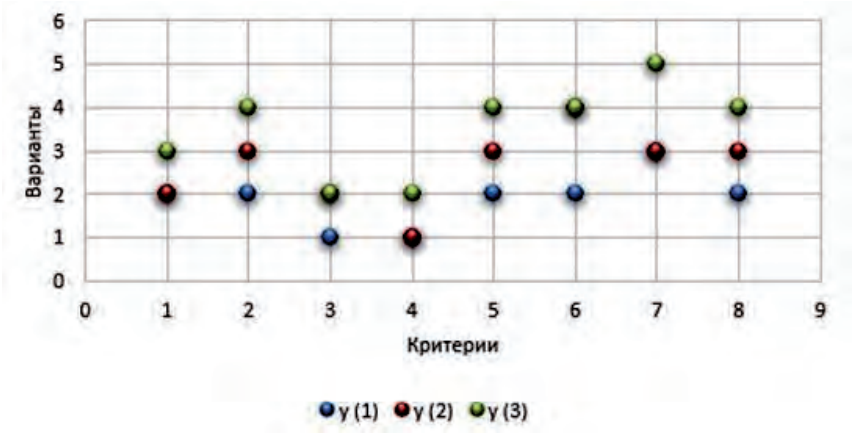

Рис.6. Диаграмма преимуществ и недостатков Методики контроля уровня защищенности информации объектов КИИ

$$f_1 \rightarrow f_1 = 5 - f_1$$
$$f_2 \rightarrow f_2 = 5 - f_2$$
$$f_3 \rightarrow f_3 = 5 - f_3$$
$$f_4 \rightarrow f_4 = 5 - f_4$$
$$f_5 \rightarrow f_5 = 5 - f_5$$
$$f_6 \rightarrow f_6 = 5 - f_6$$

Рассмотрим спецификацию вариантов:

— $y^{(1)}$ = Оценка (анализ) защищенности ИС (требования: проекты методики ФСТЭК России);

— $y^{(2)}$ = Оценка состояния защиты информации (обеспечения безопасности) в органе (организации) (требования: проект методики ФСТЭК России);

— $y^{(3)}$ = Методика контроля уровня защищенности информации объектов КИИ (требования: документы ФСТЭК России, дополнительные международные стандарты и методики).

Детальный анализ вариантов по всем критериям представлен ниже (табл.4).

Очевидно, что $y^2 \succ_y y^1$ (в силу более низкой трудоемкости, выбора уровня защищенности, показателей, частных показателей и мер защиты), а также что, в свою очередь, $y^3 \succ_y y^2$ (в силу более рационального требования к документации, «двойного» режима обеспечения безопасности КИИ, доступности технических экспертов для выполнения контроля защищенности и специалистов по ТнП, а также широкого национального и международного использования концепций и методик защищенности систем). Таким образом, вектор y^3 стоит выше над всеми иными векторами (y^2, y^1), что позволяет исключить их из множества парето-оптимальных: $y^1 \notin C(Y)$, $y^2 \notin C(Y)$. Точечная диаграмма представлена на рис.6.

Выводы

В представленной публикации предложена новая методика и рассмотрен пример практического решения задачи контроля уровня защищенности информа-

ции объектов КИИ. Выполнено сравнение по единой системе показателей представленной новой методики и доступных проектов новых методик ФСТЭК России.

Представленная методика базируется на методе «двойного режима» и вводит систему объективных и воспроизводимых численных оценок при выполнении контроля уровня защищенности информации объектов КИИ. Также методика учитывает оценки рисков (остаточных рисков), основывается на требованиях известных применимых стандартов безопасности, ставит своей целью непрерывное улучшение существующих систем защищенности информации объектов КИИ. Предложенная методика и полученные результаты могут быть применены для проведения объективного и достоверного анализа защищенности систем защищенности информации объектов КИИ.

Литература

1. Лившиц И. И., Бакшеев А.С. Исследование методик контроля уровня защищенности информации на объектах критической информационной инфраструктуры / И. И. Лившиц, А. С. Бакшеев. // Вопросы кибербезопасности. — 2022. — № 6(52). — С. 40-52.
2. Лонцих П.А., Лившиц И.И. К вопросу оценки соответствия электронных сервисов требованиям информационной безопасности на основе стандарта ISO 27001 в таможенном Союзе. — Вестник ИрГТУ. — 2015. — №11 (106). — С. 44-57.
3. Липницкий А.А., Ляшенко В.А., Пак М.А., Быковский П.С. Кибербезопасность АСУ ТП. Система верхнего блочного уровня. Базовые конфигурации кибербезопасности системного программного обеспечения // Актуальные научные исследования в современном мире. – 2020. – № 6-2 (62). – С. 62-71.
4. Ткаченко А. Кибербезопасность АСУ ТП и сертификация импортного программного и аппаратного обеспечения // Химическая техника. – 2018. – № 3. – С. 30-32.
5. Костарев С.В., Карганов В.В., Липатников В.А. Анализ угроз кибербезопасности. Проблемы информационной защиты // В книге: ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В УСЛОВИЯХ КИБЕРНЕТИЧЕСКОГО ПРОТИВОБОРСТВА. Костарев С.В., Карганов В.В., Липатников В.А. Санкт-Петербург, 2020. С. 68-93.
6. 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.
7. Kure, H.I., Islam, S. & Mouratidis, H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput & Applic 34, 15241–15271 (2022). https://doi.org/10.1007/s00521-022-06959-2
8. Eshbaev A.Kh. Theoretical Framework of Risk Management // Актуальные научные исследования в современном мире. – 2021. – № 2-7 (70). – С. 23-30.
9. Miller K.D. A Framework for Integrated Risk Management in International Business // Journal of International Business Studies. – 1992. – Т. 23. – № 2. – С. 311-331.
10. Phillips P.W.B., Smyth S. Grounding the Management of Liabilities in the Risk Analysis Framework // Bulletin of Science, Technology and Society. – 2007. – Т. 27. – № 4. – С. 274-285.
11. Maletič D., Maletič M., Pačaiová H., Nagyová A., Gomišček B. Framework Development of an Asset Manager Selection Based on Risk Management and Performance Improvement Competences // Safety. – 2021. – Т. 7. – № 1.
12. Макаренко С.И., Смирнов Г.Е. Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. №4.
13. Макаренко С. И. Тестирование на проникновение на основе стандарта NIST SP 800-115 / С.И. Макаренко. // Вопросы кибербезопасности. — 2022. — № 3(49). — С. 44-57.
14. 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.
15. Ан В.Р., Табакаева В.А. Разработка алгоритма проведения аудита кибербезопасности // В книге: МНСК-2021. Материалы 59-й Международной научной студенческой конференции. Новосибирск, 2021. С. 5.
16. Осак А.Б., Панасецкий Д.А., Бузина Е.Я. Надежность противоаварийной автоматики и релейной защиты с позиции кибербезопасности // В сборнике: Методические вопросы исследования надежности больших систем энергетики. Международный научный семинар им. Ю.Н. Руденко: В 2-х книгах. Ответственный редактор Воропай Н.И., 2018. С. 99-108.
17. Ногин В.Д. Принятие решений при многих критериях. – СПб. Издательство «ЮТАС», 2007. – 104 с.

DEVELOPMENT OF A METHODOLOGY FOR MONITORING THE LEVEL OF INFORMATION SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS

Baksheev A.S. [12]***, Livshitz I.I.*** [13]

12 Andrew S. Baksheev, student, ITMO University, St. Petersburg, Russia. E-mail: andrei.baksheev@gmail.com

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

Abstract

Purpose of work *is to increase the level of security of subjects of critical information infrastructure through the use of a "dual" regime to implement a full cycle of ensuring the security of critical information infrastructure facilities - a full national regime and a combined regime.*

Research method: *to achieve the purpose of the work, methods of analysis, comparison, generalization, structural decomposition from the theory of system analysis, determination of criteria for monitoring the level of information security of CII objects were used.*

Research result: *the paper presents a detailed analysis and comparison of existing concepts for controlling the level of information security used to obtain a certain level of security. A method for monitoring the level of information security of CII objects is proposed.*

The scientific novelty lies *in the development of a methodology for monitoring the level of information security of CII objects, using an information security audit model for CII objects, which in turn uses the possibility of a "dual mode" for a full cycle of ensuring the security of CII objects – full national and combined modes, allowing, if necessary, to include additional functional blocks.*

Keywords: *security measures, vulnerabilities, standard, risk, audit, information security, penetration testing.*

References

1. Livshits I. I., Baksheev A.S. Investigation of methods for monitoring the level of information security at critical information infrastructure facilities / I. I. Livshits, A. S. Baksheev. // Cybersecurity issues. — 2022. — № 6(52). — Pp. 40-52.
2. Lontsikh P.A., Livshits I.I. On the issue of assessing the compliance of electronic services with information security requirements based on the ISO 27001 standard in the Customs Union / P.A. Lontsikh, I.I. Livshits. — Text: direct // Bulletin of the IrSTU. — 2015. — №11 (106). — Pp. 44-57.
3. Lipnitsky A.A., Lyashenko V.A., Pak M.A., Bykovsky P.S. Cybersecurity of automated control systems. The upper block level system. Basic Cybersecurity configurations of system software // Current scientific research in the modern world. – 2020. – № 6-2 (62). – Pp. 62-71.
4. Tkachenko A. Cybersecurity of automated process control systems and certification of imported software and hardware // Chemical engineering. - 2018. – No. 3. – pp. 30-32.
5. Kostarev S.V., Karaganov V.V., Lipatnikov V.A. Analysis of cybersecurity threats. Problems of information security // In the book: INFORMATION SECURITY TECHNOLOGIES IN THE CONDITIONS OF CYBERNETIC CONFRONTATION. Kostarev S.V., Karaganov V.V., Lipatnikov V.A. St. Petersburg, 2020. pp. 68-93.
6. Robertovich A.V., Tabakaeva V.A., Selifanov V. V. Development of methods for auditing cybersecurity of state information systems related to significant objects of critical information infrastructure operating on the basis of data processing centers // Interexpo Geo-Siberia. 2020. №1.
7. Kure, H.I., Islam, S. & Mouratidis, H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. Neural Comput & Applic 34, 15241–15271 (2022). https://doi.org/10.1007/s00521-022-06959-2
8. Eshbaev A.Kh. Theoretical Framework of Risk Management // Current scientific research in the modern world. – 2021. – № 2-7 (70). – C. 23-30.
9. Miller K.D. A Framework for Integrated Risk Management in International Business // Journal of International Business Studies. – 1992. – T. 23. – № 2. – C. 311-331.
10. Phillips P.W.B., Smyth S. Grounding the Management of Liabilities in the Risk Analysis Framework // Bulletin of Science, Technology and Society. – 2007. – T. 27. – № 4. – C. 274-285.
11. Maletič D., Maletič M., Pačaiová H., Nagyová A., Gomišček B. Framework Development of an Asset Manager Selection Based on Risk Management and Performance Improvement Competences // Safety. – 2021. – T. 7. – № 1.
12. Makarenko S. I. Penetration testing based on the NIST SP 800-115 standard / S.I. Makarenko. // Cybersecurity issues. — 2022. — № 3(49). — Pp. 44-57.
13. Makarenko S.I., Smirnov G.E. Analysis of standards and methods of penetration testing // Control systems, communications and security. 2020. №4.
14. Nesterovsky O.I., Pashkovskaya E.S., Butrik E.E. Methodical approach to the organization of information security control at critical information infrastructure facilities // Bulletin of the Ministry of Internal Affairs of Russia. - 2021. — No. 2. — pp.126-133
15. An V.R., Tabakaeva V.A. Development of an algorithm for conducting a cybersecurity audit // In the book: MNSK-2021. Materials of the 59th International Scientific Student Conference. Novosibirsk, 2021. P. 5.
16. Osak A.B., Panasetsky D.A., Buzina E.Ya. Reliability of emergency automation and relay protection from the standpoint of cybersecurity // In the collection: Methodological issues of reliability research of large energy systems. International Scientific Seminar named after Y.N. Rudenko: In 2 books. Responsible editor Voropai N.I., 2018. pp. 99-108.
17. V.D. Nogin. Decision-making under many criteria. – St. Petersburg. UTAS Publishing House, 2007. – 104 p.