ISSN 2782-2001
Системы анализа и обработки данных
том 89, № 1, 2023, с. 37–54

http://journals.nstu.ru/vestnik
Analysis and data processing systems
Vol. 89, No. 1, 2023, pp. 37–54

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

INFORMATION TECHNOLOGIES AND TELECOMMUNICATIONS

УДК 004.056

DOI: 10.17212/2782-2001-2023-1-37-54

Анализ стандартов обеспечения информационной безопасности*

Д.В. КЛИШИН[1,a], А.А. ЧЕЧУЛИН[2,b]

[1] *197101, РФ, г. Санкт-Петербург, Кронверкский проспект, 49А, Национальный исследовательский университет ИТМО*
[2] *199178, Россия, г. Санкт-Петербург, 14-я линия, 39, Санкт-Петербургский федеральный исследовательский центр Российской академии наук*

[a] *dvklishin@itmo.ru* [b] *andreych@bk.ru*

Целью работы является систематизация имеющихся знаний о моделях информационной безопасности, представленных в стандартах и научных исследованиях для решения проблемы трудоемкости: анализа и выбора актуальной для информационной инфраструктуры предприятия модели информационной безопасности, оценки текущего уровня информационной безопасности предприятия.

При выявлении и анализе использующихся моделей информационной безопасности в рамках настоящей работы рассмотрены стандарты, нормативные правовые акты и научные исследования в области информационной безопасности. Систематизация знаний о моделях информационной безопасности производилась с помощью анализа стандартов, научных исследований, нормативных правовых актов по информационной безопасности; выявления общих свойств моделей информационной безопасности; группировки критериев и свидетельств, подтверждающих реализацию мер информационной безопасности, по общим признакам; выявления способов автоматизации оценки текущего уровня информационной безопасности.

В ходе работы выявлены основные критерии модели информационной безопасности; сформирован перечень свидетельств, позволяющих контролировать реализацию мер информационной безопасности; выявлены общие признаки критериев, свидетельств, достаточных для группирования; выявлены виды свидетельств; сформирован алгоритм оценки текущего уровня информационной безопасности предприятия; выявлены способы автоматизации сбора информации об используемой предприятием модели информационной безопасности и свидетельств реализации мер информационной безопасности.

Настоящая работа систематизирует знания о существующих моделях и позволяет проанализировать критерии информационной безопасности без необходимости изучения всех рассмотренных в статье стандартов и научных работ, что позволяет сократить трудоемкость анализа и выбора актуальной для информационной инфраструктуры предприятия модели информационной безопасности. Результаты настоящей работы будут применены для выявления возможности автоматизации оценки текущего уровня информационной безопасности предприятия.

* *Статья получена 20 сентября 2022 г.*

Ключевые слова: информационная безопасность, уровень информационной безопасности, оценка уровня информационной безопасности, модель информационной безопасности, критерии информационной безопасности, свидетельства, требования, стандарты

ВВЕДЕНИЕ

Организация информационной безопасности на предприятии начинается с определения актуальных рисков и угроз информационной безопасности для информационной инфраструктуры предприятия. При применении проактивного подхода к управлению процессами информационной безопасности требуется выбрать и реализовать меры информационной безопасности, позволяющие снизить или устранить актуальные риски и угрозы информационной безопасности. В качестве проактивного инструмента, позволяющего подобрать необходимый набор мер информационной безопасности под определенные риски и угрозы информационной безопасности, разработаны модели информационной безопасности.

Под моделью информационной безопасности подразумеваются требования к совокупности технических и организационных мер по обеспечению информационной безопасности, а также требования к объектам и процессам информационной безопасности. Структура модели состоит из мер информационной безопасности, сгруппированных по общим признакам – критериям. Реализация данных мер необходима для снижения или устранения определенных рисков, угроз информационной безопасности и достижения требуемого уровня информационной безопасности на предприятии.

Модели информационной безопасности представлены нормативными правовыми актами, международными стандартами, научными исследованиями и требованиями для определенных сфер финансового и промышленного рынка.

Таким образом, в представленной работе рассматриваются существующие отечественные и зарубежные варианты моделей информационной безопасности, ставится вопрос об объеме выборки мер и критериев модели информационной безопасности, а также формируется перечень свидетельств, необходимых для доказательства реализации мер информационной безопасности.

1. ПОСТАНОВКА ЗАДАЧИ

В настоящее время в области информационной безопасности имеется много моделей информационной безопасности. Большинство из этих моделей информационной безопасности имеют схожие или общие меры и критерии, помимо этого, они имеют уникальные для каждой модели информационной безопасности особенности.

В случаях, когда выбор подходящей модели информационной безопасности не определен требованиями законодательства и регуляторов отрасли, то подбор актуальной для информационной инфраструктуры предприятия модели информационной безопасности является трудоемкой задачей. Выбор необходимой модели информационной безопасности также может потребоваться для компенсирования мер, не рассматриваемых в моделях, определенных требованиями нормативных правовых актов.

Научная новизна данной работы заключается в предложении методики проведения оценки соответствия реальных показателей уровня информационной безопасности организации требованиям стандартов, нормативных правовых актов и руководящих документов в области ИБ, представленных моделями информационной безопасности; в статье предложены способы автоматизации процессов, описанных в методике.

Для достижения цели работы необходимо следующее: провести литературный обзор стандартов, нормативных правовых актов и научных исследований по информационной безопасности для выявления моделей информационной безопасности; проанализировать модели информационной безопасности, представленные в стандартах, нормативных правовых актах и научных исследованиях; систематизировать полученные знания путем выявления общих свойств для моделей информационной безопасности; выявить и систематизировать критерии моделей и свидетельства, подтверждающие реализацию мер информационной безопасности; выявить возможные способы автоматизации сбора свидетельств реализации мер информационной безопасности.

2. МАТЕРИАЛЫ И МЕТОДЫ

Согласно исследованию организации Compliance Forge [11], на международном рынке ИБ насчитывается более 180 нормативных правовых актов и стандартов, описывающих модели информационной безопасности.

При выявлении и анализе использующихся моделей в рамках настоящей работы были рассмотрены следующие документы по информационной безопасности:

– нормативная правовая документация ФСТЭК России [1–4];
– стандарты ГОСТ Р ИСО/МЭК серии 27 [5–7];
– серия стандартов NIST [8–10];
– стандарт PCI DSS [12];
– научные исследования в области информационной безопасности, в том числе фреймворки [11, 13, 14].

Также помимо стандартов, описывающих модели, были проанализированы работы [14, 15], описывающие методы оценки соответствия текущего уровня информационной безопасности с моделью, описанной в стандартах.

В рамках настоящей работы рассматривались только базовые наборы мер по обеспечению информационной безопасности, представленные в рассматриваемых документах, с целью определения объема выборки критериев и мер. Определение объема выборки критериев и мер каждого документа требуется для выявления пересечений множеств мер информационной безопасности, что позволяет определить общие и различные для каждой модели меры и критерии информационной безопасности и на основе полученной информации выявить перечень свидетельств, подтверждающих реализацию мер.

В ходе оценки документов по информационной безопасности были выявлены критерии моделей информационной безопасности. Количество критериев и мер представлено в табл. 1.

3. РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

В рамках работы было выявлено, что большинство из рассмотренных моделей информационной безопасности имеют схожие или общие меры и критерии, также они имеют уникальные особенности.

В ходе анализа моделей информационной безопасности было выявлено, что модели имеют следующие отличительные признаки:

– детализация мер информационной безопасности;
– объем выборки критериев информационной безопасности;
– рассматриваемые угрозы и риски информационной безопасности;
– подход к обеспечению информационной безопасности.

Таблица 1

Table 1

Критерии моделей информационной безопасности

Criteria of information security models

№ п/п	Наименование стандарта	Критерии
1	Серия стандартов ГОСТ Р ИСО/МЭК: ГОСТ Р ИСО/МЭК 27000–2021 [5] ГОСТ Р ИСО/МЭК 27001–2021 [6] ГОСТ Р ИСО/МЭК 27002–2021 [7]	Количество критериев: 14. Количество мер информационной безопасности: 114
		Стандартом не предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации осуществляется для всех мер информационной безопасности
2	Серия стандартов NIST Special Publication: 800-53 Revision 5 [8] 800-53A Revision 5 [9] 800-53B Revision 5 [10]	Количество критериев: 20. Количество мер информационной безопасности: >256
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории. Процесс оценки использует три категории, основанные на возможном воздействии на информационную инфраструктуру. К каждому уровню воздействия должен применяться свой набор мер
3	NIST Framework for Improving Critical Infrastructure Cybersecurity [11]	Количество критериев: 22. Количество мер информационной безопасности: 98
		Стандартом не предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации осуществляется для всех мер информационной безопасности

Продолжение табл. 1

Continuon of Tab. 1

№ п/п	Наименование стандарта	Критерии
4	Payment Card Industry Data Security Standard. Requirements and Testing Procedures (PCI DSS) [12]	Количество критериев: 12. Количество мер информационной безопасности: 288
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории. Категория выбирается по признакам значимости информационной инфраструктуры (по количеству транзакций)
5	Приказ ФСТЭК России № 17 от 11.02.2013 г. [1]	Количество критериев: 17. Количество мер информационной безопасности: 151
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории. Набор мер выбирается в зависимости от класса защищенности информационной системы, который зависит от масштаба информационной системы
6	Приказ ФСТЭК России № 21 от 18.02.2013 г. [2]	Количество критериев: 15. Количество мер информационной безопасности: 109
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории. Набор мер выбирается в зависимости от уровня защищенности персональных данных, который зависит от категории, вида и угроз, обрабатываемых персональных данных
7	Приказ ФСТЭК России № 239 от 25.12.2017 г. [3]	Количество критериев: 13. Количество мер информационной безопасности: 113
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории. Набор мер выбирается в зависимости от категории значимости информационной инфраструктуры

Окончание табл. 1

End of Tab. 1

№ п/п	Наименование стандарта	Критерии
8	Secure Controls Framework (SFC) [13]	Количество критериев: 32. Количество мер информационной безопасности: 1058
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории
9	A framework and theory for cyber security assessments [14]	Количество критериев: 22. Количество мер информационной безопасности: 102. Отношения между критериями: 51
		Стандартом предусмотрено категорирование информационной инфраструктуры для определения наиболее подходящего для предприятия набора мер, в связи с чем оценка реализации мер осуществляется в зависимости от выбранной категории

С учетом вышеперечисленных отличительных признаков анализ моделей информационной безопасности позволил выявить схожесть и различия разных моделей. Для выполнения целей и задач, поставленных в рамках настоящей работы, требуется выбрать документ по информационной безопасности, включающий в себя наибольший объем выборки критериев и мер информационной безопасности.

В рамках настоящей статьи в качестве работы, в которой представлен наибольший объем выборки критериев и мер информационной безопасности, было выбрано исследование Secure Controls Framework [13], включающее в себя анализ более 184 стандартов и исследований, из которых взяты и объединены общие критерии, а также представлены уникальные для каждого стандарта исследования, что позволило сократить общее количество мер. Схематическое изображение объема выборки стандартов, нормативных правовых актов и исследований представлено на рис. 1.

В ходе анализа критериев модели информационной безопасности, представленных в исследовании Secure Controls Framework [13], была выявлена необходимость сокращения количества критериев модели путем объединения схожих по описанию и назначению критериев. Критерии, выбранные для объединения, представлены в табл. 2.

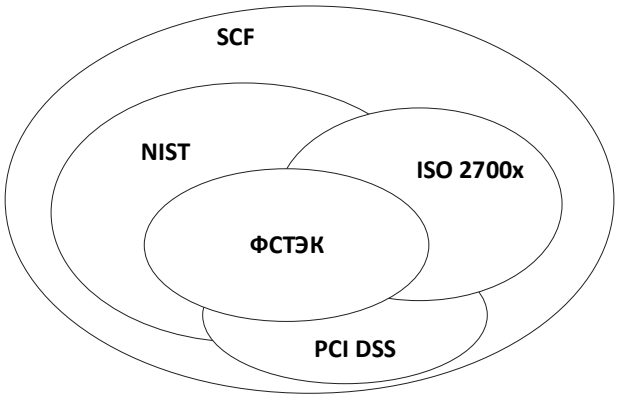

Рис. 1. Схематическое изображение объема выборки рассмотренных работ

Fig. 1. Schematic representation of the sample size of the considered works

Ниже представлен итоговый перечень критериев, выбранных для систематизации в рамках настоящей работы:

– организация и управление деятельностью по информационной безопасности (GOV);
– безопасная разработка (TDA);
– риск-ориентированный подход (RTV);
– обеспечение доступности (CAP);
– кадровая безопасность (HRS);
– соответствие правовым и договорным требованиям (CPL);
– обработка и категорирование информации (DCH);
– управление активами (AST);
– управление конфигурацией (CFG);
– управление изменениями (CHG);
– мониторинг информационной безопасности (MON);
– реагирование на инциденты информационной безопасности (IRO);
– архитектура информационной безопасности (SEA);
– защита информационной инфраструктуры и компонентов (NET);
– криптографическая защита информации (CRY);
– защита рабочих мест (END);
– идентификация и аутентификация (IAC);
– выявление нерегламентированных функциональных характеристик (EMB);
– контроль за использованием мобильных устройств и носителей информации (MDM);
– управление уязвимостями и обновлениями (VPM);
– физическая безопасность (PES);
– безопасность персональных данных (PRI).

Таблица 2

Table 2

Критерии Secure Controls Framework, выбранные для объединения

Secure Controls Framework Criteria selected for integration

№ п/п	Объединяемые критерии	Причина объединения	Наименование нового критерия
1	Организация и управление деятельностью по информационной безопасности (GOV). Управление проектами по информационной безопасности (PRM). Обеспечение информационной безопасности (OPS)	Все меры из указанных критериев относятся к верхнеуровневой административной деятельности по информационной безопасности и имеют общие признаки	Организация и управление деятельностью по информационной безопасности (GOV)
2	Обеспечение безопасности облачных сервисов (CLD). Контроль выполнения мер информационной безопасности (IAO). Безопасная разработка (TDA). Безопасность веб-приложений (WEB)	Все меры из указанных критериев относятся к использованию предприятием программного обеспечения, программный код которого разработан работниками предприятия	Безопасная разработка (TDA)
3	Управление рисками (RSK). Управление угрозами (THR)	Все меры из указанных критериев относятся к применению риск-ориентированного подхода	Риск-ориентированный подход (RTV)
4	Непрерывность бизнес-процессов и восстановление информационной инфраструктуры (BCD). Обеспечение доступности (CAP). Обслуживание информационной инфраструктуры (MNT)	Все меры из указанных критериев относятся к риск-ориентированному подходу и имеют общие признаки для группирования	Обеспечение доступности (CAP)
5	Кадровая безопасность (HRS). Обучение персонала (SAT)	Все меры из указанных критериев относятся к обеспечению свойства доступности информации, обрабатываемой / хранящейся информационной инфраструктурой предприятия	Кадровая безопасность (HRS)
6	Соответствие правовым и договорным требованиям (CPL). Управление взаимодействиями с подрядчиками и поставщиками (TPM)	Административная часть мер из указанных критериев относится к деятельности отдела кадров	Соответствие правовым и договорным требованиям (CPL)

Поскольку основной целью информационной безопасности является предоставление безопасного доступа легитимных субъектов к объектам информационной инфраструктуры, будет закономерно систематизировать выявленные критерии информационной безопасности по уровням реализации механизмов безопасности, по целям и функциональным категориям.

При анализе перечня критериев, выбранных для систематизации, было выявлено, что критерии можно условно распределить между четырьмя группами.

1. Политика информационной безопасности, включающей в себя критерии, относящиеся к верхнеуровневым, организационным мерам, позволяющим планировать и управлять процессами информационной безопасности.

2. Контроль информационной безопасности, включающей в себя критерии, относящиеся к контролю организации и мониторингу информационной безопасности.

3. Система защиты, включающей в себя критерии, относящиеся средствам и системам защиты информации.

4. Безопасность системы, включающей в себя критерии, относящиеся к безопасному функционированию системы.

Анализ мер информационной безопасности из выбранных для систематизации критериев позволил сформировать и систематизировать перечень свидетельств, необходимых для контроля за выполнением мер информационной безопасности.

Выявленные свидетельства можно разделить на четыре группы.

1. Организационно-распорядительная документация – все свидетельства, относящиеся к документации, связанной с административно-бытовой деятельностью предприятия.

2. Информация об информационной инфраструктуре – все свидетельства, относящиеся к информации, связанной с информационными технологиями, используемыми в информационной инфраструктуре предприятия.

3. Документация по информационной безопасности – все свидетельства, относящиеся к документации, связанной с информационной безопасностью.

4. Информация о средствах защиты информации – все свидетельства, относящиеся к информации о наличии средств защиты информации, автоматизирующих процессы управления ИБ, а также их конфигурации.

К группе «Организационно-распорядительная документация» относятся следующие свидетельства: протоколы обучения работников; результаты проверки знаний работников; приказы о назначении работников на должности, связанные с обслуживанием информационной инфраструктуры; кадровая документация и записи о профессиональных компетенциях; схема организационной структуры предприятия; договоры с подрядными организациями по части обслуживания и доступа к информационной инфраструктуре; документация о территории, принадлежащей предприятию на праве собственности или аренды; договоры с провайдерами интернет-услуг или услуг по предоставлению вычислительных мощностей; информация по обучению сотрудников использованию и обслуживанию информационной инфраструктуры и отчетность по итогам; планы действий по непрерывности и восстановлению бизнес-процессов.

К группе «Информация об информационной инфраструктуре» относятся следующие свидетельства: наличие альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций; результаты инструментальных сканирований объектов информационной инфраструктуры; конфигурация активов информационной инфраструктуры; инвентарная опись активов информационной инфраструктуры с их описанием; схема информационной инфраструктуры; верхнеуровневые политики, положения, регламенты и стандарты, регламентирующие процессы информационной безопасности; документы, описывающие требования и порядок реализации процедур по информационной безопасности; перечень конфиденциальной информации; перечень критической информационной инфраструктуры; отчеты о мониторинге информационной безопасности; матрицы доступа; журнал учета машинных носителей информации; журнал безопасности доступа к носителям информации; информация об отказоустойчивости информационной инфраструктуры; информация об энергозависимости информационной инфраструктуры; перечень отказоустойчивых технических средств; перечень энергозависимых технических средств, которым необходимо обеспечить наличие резервных источников питания.

К группе «Документация по информационной безопасности» относятся следующие свидетельства: верхнеуровневые политики, положения, регламенты, стандарты (регламентирующие планирование процессов по обеспечению защиты информации; порядок действий в нештатных ситуациях; порядок обучения пользователей; правила предотвращений вторжений; правила проведения аудита; выявление и устранение уязвимостей; обеспечение доступности; правила управления обновлениями; обеспечение целостности; резервное копирование информации; физическую защиту технических средств); низкоуровневые документы, процедуры, стандарты и т. п. (описывающие требования и порядок организации деятельности по информационной безопасности; оценки риска и угроз; предотвращения вторжений; выявления уязвимостей; определения источника времени; сбора и хранения информации о событиях безопасности; проведения внутренних аудитов; проведения внешних аудитов); политика информационной безопасности; дорожная карта / планы развития информационной безопасности; модель угроз информационной безопасности; отчеты об оценке рисков; методика оценки рисков; план мероприятий по обеспечению защиты информации; план действий в нештатных ситуациях; протоколы отработки действий в нештатных ситуациях; результаты сканирований, пентестов, штабных киберучений и киберучений; отчеты о проведении внешних и внутренних аудитов; журнал событий безопасности; критические сегменты информационной инфраструктуры; категорирование информации; перечни разрешенных действий и разрешенного программного обеспечения и операционных систем; журнал резервного копирования; журнал восстановления информации; перечень компонентов программного обеспечения, разрешенных к установке; реестр доверенных источников для получения обновлений ПО.

К группе «Информация о средствах защиты информации» относится информация о средствах защиты информации, позволяющих автоматизировать предотвращение компьютерных атак; выявление уязвимостей; синхронизацию системного времени; процесс сбора, записи, хранения, учета событий безопас-

ности в журнале событий безопасности; процесс анализа действий отдельных пользователей; процессы управления доступом пользователей; процессы управления учетными записями пользователей; процессы управления парольной политикой; защиту аутентификационной информации при ее передаче; антивирусную защиту; процессы учета машинных носителей информации; уничтожение (стирание) информации; выявление компьютерных инцидентов; резервирование средств и систем; контроль безотказного функционирования средств и систем; обеспечивающие резервное копирование информации; восстановление информации; управление изменениями конфигурации программного обеспечения; установку только разрешенного к использованию программного обеспечения; поиск и получение обновлений программного обеспечения; контроль целостности обновлений на предмет ошибок, вирусов, встроенных программных закладок; процессов обновления программного обеспечения.

В результате анализа групп свидетельств можно выделить три вида свидетельств: 1) документальные свидетельства – свидетельства, полученные из документов предприятия; 2) программные свидетельства – свидетельства, полученные от программного обеспечения; 3) аудиторские свидетельства – свидетельства, полученные при аудиторской проверке.

Варианты автоматизации процесса сбора свидетельств реализации мер информационной безопасности представлены в табл. 3.

Таблица 3

Table 3

Виды свидетельств

Types of evidences

Документальные свидетельства	Свидетельства, собранные аудитором	Свидетельства, полученные от ПО
– Анализ наличия документов, наличия их пересмотра и обновлений путем анализа метаданных всех версий документов – Поиск информации в документах по ключевым словам – Приведение всех документов по информационной безопасности к единому формату, который позволяет сконвертировать информацию о мерах в документы формата json, csv и т. п. – Перечень активов и их конфигураций в формате json	– Подключение к интерфейсам программного обеспечения, таким как REST API или другим API – Получение конфигураций программного обеспечения, средств защиты информации, аппаратно-программных комплексов из централизованных систем управления, таких как Active Directory, Kaspersky Security Center, сетевых хранилищ (NAS), MaxPatrol SIEM и т. п. – Выгрузка организационной информации о предприятии из такого программного обеспечения, как 1С и Active Directory в форматах json, csv – Сбор информации аудитором в документ, который позволяет сконвертировать информацию о мерах в документы формата json, csv и т. п.	Получение актуальной информации о сети за счет анализа результатов автоматизированного инструментального сканирования программного обеспечения и средств защиты информации

В качестве долгосрочной перспективы использования программного обеспечения для автоматизации оценки текущего уровня информационной безопасности можно рассмотреть вариант формирования модели информационной безопасности за счет:

– приведения всех документов по информационной безопасности к единому формату, который позволяет сконвертировать информацию об используемых мерах в документы формата json, csv и т. п.;

– предоставления перечня активов и их конфигураций в формате json, csv и т. п.

В случаях, когда автоматизированный сбор информации невозможен, аудитор может самостоятельно создавать объекты информационной инфраструктуры из предложенных шаблонов и заполнять поля их значений.

Целью выявления вариантов автоматизации сбора свидетельств является снижение объема трудозатрат на оценку соответствия внутренних показателей предприятия эталонным моделям информационной безопасности. Оценка соответствия внутренних показателей предприятия эталонным моделям информационной безопасности позволит определить текущий уровень информационной безопасности предприятия и повысить его за счет реализации мер информационной безопасности, описанных в эталонной модели, но не реализованных ранее. Для оценки соответствия внутренних показателей предприятия эталонным моделям информационной безопасности может быть использована методика, представленная на рис. 2.

Рис. 2. Методика оценки текущего уровня информационной безопасности

Fig. 2. Methodology for assessing the current level of information security

Данная методика может быть применена в программном обеспечении, которое позволит выполнить комплексную оценку текущего уровня информационной безопасности предприятия. Определение текущего уровня информационной безопасности предполагается за счет оценки соответствия модели текущего уровня и модели, выбранной предприятием в качестве эталонной для обеспечения информационной безопасности.

Для определения модели, выбранной предприятием в качестве эталонной, необходимо проанализировать организационно-распорядительную документацию предприятия в области информационной безопасности предприятия или выбрать модель из стандартов и нормативных правовых актов.

Для автоматизации сбора информации об используемой на предприятии модели информационной безопасности можно рассмотреть варианты, представленные в табл. 4.

Таблица 4

Table 4

Информация об используемой модели

Information on the model used

Из организационно-распорядительной информации	Выбор параметров модели	Выбор модели
– Автоматический поиск по ключевым словам в политике информационной безопасности и верхнеуровневых документах по информационной безопасности – Поиск информации по ключевым словам о параметрах модели информационной безопасности в проектной документации, инструкциях пользователей и администраторов, низкоуровневых регламентах, описывающих настройки – Формирование модели информационной безопасности за счет приведения документации к единому формату, который позволяет сконвертировать информацию о мерах в документы формата json, csv и т. п.	Аудитор самостоятельно выбирает параметры модели информационной безопасности, дополняя шаблоны моделей или модели, сформированные после автоматизированного анализа документов по информационной безопасности	Аудитор выбирает готовые шаблоны моделей информационной безопасности, сформированные на основе нормативных правовых документов и международных стандартов

В качестве долгосрочной перспективы использования программного обеспечения для автоматизации оценки текущего уровня информационной безопасности можно рассмотреть вариант формирования модели за счет приведения документации к единому формату, который позволяет сконвертировать информацию о мерах в документы формата json, csv и т. п.

Оценка текущего уровня информационной безопасности предприятия является комплексной и включает в себя определение реализованных мер информационной безопасности для всех объектов информационной инфраструктуры. Поскольку для разных объектов информационной инфраструктуры предприятия требуется реализовывать разный набор мер, то при формировании эталонной модели информационной безопасности, которую использует предприятие, требуется использовать объектно ориентированные методы моделирования. Также поскольку у типовых объектов информационной инфраструктуры может быть использован разный набор мер информационной безопасности или набор мер, отличный от набора мер эталонной модели информационной безопасности, то в случае моделирования текущего уровня информационной безопасности предприятия требуется использовать объектно ориентированные методы моделирования.

ЗАКЛЮЧЕНИЕ

В рамках данной статьи были рассмотрены стандарты, нормативные правовые акты и научные исследования в области информационной безопасности, что позволило выявить основные критерии модели информационной безопасности; сформировать перечень свидетельств, позволяющих контролировать реализацию мер информационной безопасности; выявить общие признаки критериев и свидетельств, достаточных для группирования и систематизации; выявить виды свидетельств; сформировать методику оценки текущего уровня информационной безопасности предприятия; выявить способы автоматизации сбора информации об используемой предприятием модели информационной безопасности и свидетельств реализации мер информационной безопасности.

В работе выявлены общие для каждого рассматриваемого стандарта критерии и свидетельства, что позволило разработать методику оценки текущего уровня информационной безопасности, а также систематизировать имеющиеся знания о моделях информационной безопасности и решить проблемы трудоемкости анализа и выбора актуальной для информационной инфраструктуры предприятия модели информационной безопасности.

Исходя из полученной информации можно сделать вывод, что наилучшим принципом, лежащим в основе программного обеспечения, позволяющего автоматизировать оценку текущего уровня информационной безопасности предприятия, является формирование моделей объектов информационной инфраструктуры предприятия и присвоение им характеристик, описанных в стандартах, нормативных правовых актах и организационно-распорядительной документации в области информационной безопасности предприятия. Затем требуется сформировать модели объектов информационной инфраструктуры и присвоить им характеристики, соответствующие актуальным на момент проведения аудита, далее сравнить данные модели объектов.

В качестве примера реализации программного обеспечения, создающего модели объектов информационной инфраструктуры, можно взять программное обеспечение Maltego, Bloodhound.

Выявленные критерии информационной безопасности позволят сформировать наиболее актуальный перечень мер, пункты которого не будут повторяться и будут соответствовать моделям информационной безопасности, рассматриваемым в современных исследованиях и стандартах по информационной безопасности. Сформированный перечень свидетельств позволит разработать способ автоматизации контроля реализации мер информационной безопасности. Автоматизация процесса контроля реализации мер информационной безопасности позволит уменьшить трудоемкость процесса выявления текущего уровня информационной безопасности у предприятий за счет сравнения модели информационной безопасности, используемой предприятием, и фактически реализованных мер.

Работа выполнена при частичной финансовой поддержке гранта РФФИ 19-29-06099-мк.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (дата обращения: 03.03.2023).

2. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 03.03.2023).

3. Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». – URL: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения: 03.03.2023).

4. Методический документ Федеральной службы по техническому и экспортному контролю от 11 февраля 2014 г. «Меры защиты информации в государственных информационных системах». – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (дата обращения: 03.03.2023).

5. ГОСТР ИСО/МЭК 27000–2021. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология: взамен ГОСТ Р ИСО/МЭК 27000–2012: дата введения 2021–11–30. – М.: Рос. ин-т стандартизации, 2021. – 28 с.

6. ГОСТ Р ИСО/МЭК 27001–2021. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: взамен ГОСТ Р ИСО/МЭК 27001–2006: введ. 2022–01–01. – М.: Рос. ин-т стандартизации, 2021. – 23 с.

7. ГОСТ Р ИСО/МЭК 27002–2021. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности: взамен ГОСТ Р ИСО/МЭК 27002–2012: введ. 2021–11–30. – М.: Рос. ин-т стандартизации, 2021. – 68 с.

8. NIST SP 800-53 Rev. 5. Security and privacy controls for information systems and organizations: – September 2020. – 492 p.

9. NIST SP 800-53A Rev. 5. Security and privacy controls for Information systems and organizations: – January 2022. – 733 p.

10. NIST SP 800-53B Rev. 5. Security and privacy controls for information systems and organizations. – October 2022. – 85 p.

11. Framework for improving critical infrastructure cybersecurity. Version 1.1 / National Institute of Standards and Technology. – NIST, April 16, 2018. – 55 p.

12. Payment Card Industry Data Security Standard (PCI DSS). Requirements and Security Assessment Procedures. Version 3.2.1. – May 2018. – 139 p.

13. Secure Controls Framework: website. – URL: https://www.securecontrolsframework.com/ (accessed: 03.03.2023).

14. *Sommestad T.* A framework and theory for cyber security assessments: Dr. of Philosophy diss. / Royal Institute of Technology. – Stockholm, Sweden, 2012. – 248 p.

15. Проблемные вопросы информационной безопасности киберфизических систем / Д.С. Левшун, Д.А. Гайфулина, А.А. Чечулин, И.В. Котенко // Информатика и автоматизация. – 2020. – Т. 19, № 5. – С. 1050–1088.

16. Choosing models for security metrics visualization / M. Kolomeec, G. Gonzalez-Granadillo, E. Doynikova, A. Chechulin, I. Kotenko, H. Debar // Computer Network Security. MMM-ACNS 2017. – Springer-Verlag, 2017. – P. 75–87. – (Lecture Notes in Computer Science; vol. 10446).

Клишин Данил Владимирович, аспирант Федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет ИТМО». Основное направление научных исследований – информационная безопасность. E-mail: dvklishin@itmo.ru

Чечулин Андрей Алексеевич, кандидат технических наук, доцент, ведущий научный сотрудник лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский федеральный исследовательский центр Российской академии наук». Основное направление научных исследований – информационная безопасность. E-mail: andreych@bk.ru

Klishin Danil V., a post-graduate student, Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics. His research interests are currently focused on information security. E-mail: dvklishin@itmo.ru

Chechulin Andrey A., PhD (Eng.), an associate professor, St. Petersburg Federal Research Center of the Russian Academy of Sciences. His research interests are currently focused on information security. E-mail: andreych@bk.ru.

DOI: 10.17212/2782-2001-2023-1-37-54

Analysis of information security standards[*]

D.V. KLISHIN[1,a], *A.A. CHECHULIN*[2,b]

[1] *Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics, Kronverksky Prospekt 49, bldg. A, St. Petersburg, 197101, Russian Federation*

[2] *St. Petersburg Federal Research Center of the Russian Academy of Sciences, 14 liniya, 39, St, Petersburg, 199178, Russian Federation*

[a] *dvklishin@itmo.ru* [b] *andreych@bk.ru*

Abstract

The purpose of the work is to systematize the available knowledge about information security models presented in standards and scientific research to solve the problem of labor intensity: analysis and selection of an information security model relevant to the information infrastructure of the enterprise; and assessment of the current level of information security of the enterprise.

When in identifying and analyzing the information security models used, standards, regulatory legal acts and scientific research in the field of information security are considered within the framework of this work. The systematization of knowledge about information security models was carried out with the help of analysis of standards, scientific research, normative legal acts on information security; identifying common properties of information security models; grouping criteria and evidence confirming the implementation of information security measures by common signs; identifying ways to automate the assessment of the current level of information security.

In the course of the work: the main criteria of the information security model were identified; a list of certificates was formed that allow monitoring the implementation of information security measures; common features of criteria, certificates sufficient for grouping were revealed; types of certificates were identified; an algorithm for assessing the current level of information security of an enterprise was formed; methods of automatization of collecting information about models of information security used by an enterprise and evidence of the implementation of information security measures were identified .

This work systematizes knowledge about the existing models and allows analyzing the criteria of information security without a need to study all the standards and scientific papers

[*] *Received 20 September 2022.*

considered in this work, which reduces the labor intensity of the analysis and selection of an information security model relevant to the information infrastructure of an enterprise. The results of this work will be applied to identify the possibility of automating the assessment of the current level of information security of an enterprise.

Keywords: information security, information security level, information security level assessment, information security model, information security criteria, certificates, requirements, standards

REFERENCES

1. Order of the FSTEC of Russia No. 17 dated February 11, 2013 “On the approval of the Requirements for the protection of information that does not constitute a state secret contained in state information systems”. (In Russian). Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (accessed 03.03.2023).

2. Order of the FSTEC of Russia No. 21 dated February 18, 2013 “On the approval of the Composition and content of organizational and technical measures to ensure the security of personal data during their processing in personal data information systems”. (In Russian). Available at: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed 03.03.2023).

3. Order of the FSTEC of Russia No. 239 dated December 25, 2017 “On approval of requirements for ensuring the security of significant objects of critical information infrastructure of the Russian Federation”. (In Russian). Available at: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (accessed 03.03.2023).

4. Methodical document of the FSTEC of Russia dated February 11, 2014 “Information protection measures in state information systems”. (In Russian). Available at: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument (accessed 03.03.2023).

5. GOST ISO/MEK 27000–2021. *Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoi bezopasnosti. Obshchii obzor i terminologiya* [State standard GOST R ISO/MEK 27000–2021. Information technology. Security techniques. Information security management systems. Overview and vocabulary]. Moscow, Russian Standardization Institute Publ., 2021. 28 p.

6. GOST R ISO/MEK 27001–2021. *Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoi bezopasnosti. Trebovaniya* [State standard GOST R ISO/MEK 27001–2021. Information technology. Security techniques. Information security management systems. Requirements]. Moscow, 2021. 23 p.

7. GOST ISO 27002–2021. *Metody i sredstva obespecheniya bezopasnosti. Svod norm i pravil primeneniya mer obespecheniya informatsionnoi bezopasnosti* [State standard GOST ISO 27002–2021. Information technology. Security techniques. Code of practice for information security controls]. Moscow, 2021. 68 p.

8. NIST SP 800-53 Rev. 5. *Security and privacy controls for information systems and organizations*. September 2020. 492 p.

9. NIST SP 800-53A Rev. 5. *Security and privacy controls for Information systems and organizations*. January 2022. 733 p.

10. NIST SP 800-53B Rev. 5. *Security and privacy controls for information systems and organizations*. October 2022. 85 p.

11. NIST. *Framework for Improving Critical Infrastructure Cybersecurity*. Version 1.1. April 16, 2018. 55 p.

12. Payment Card Industry Data Security Standard (PCI DSS). *Requirements and Security Assessment Procedures*. Version 3.2.1. May 2018. 139 p.

13. Secure Controls Framework. Website. Available at: https://www.securecontrolsframework.com/ (accessed 03.03.2023).

14. Sommestad T. *A framework and theory for cyber security assessments*. Dr. of Philosophy diss. Royal Institute of Technology. Stockholm, Sweden, 2012. 248 p.

15. Levshun D., Gaifulina D., Chechulin A., Kotenko I. Problemnye voprosy informatsionnoi bezopasnosti kiberfizicheskikh sistem [Problematic issues of information security of cyber-physical systems]. *Informatika i avtomatizatsiya = Informatics and Automation*, 2020, vol. 19, no. 5, pp. 1050–1088.

16. Kolomeec M., Gonzalez-Granadillo G., Doynikova E., Chechulin A., Kotenko I., Debar H. Choosing models for security metrics visualization. Computer Network Security. MMM-ACNS 2017. Springer-Verlag, 2017, pp. 75–87.

Для цитирования:

Клишин Д.В., Чечулин А.А. Анализ стандартов обеспечения информационной безопасности // Системы анализа и обработки данных. – 2023. – № 1 (89). – С. 37–54. – DOI: 10.17212/2782-2001-2023-1-37-54.

For citation:

Klishin D.V., Chechulin A.A. Analiz standartov obespecheniya informatsionnoi bezopasnosti [Analysis of information security standards]. *Sistemy analiza i obrabotki dannykh = Analysis and Data Processing Systems*, 2023, no. 1 (89), pp. 37–54. DOI: 10.17212/2782-2001-2023-1-37-54.