Способ сетевого планирования аудита информационной безопасности объектов критической информационной инфраструктуры

Н. Е. Платов, email: platovne@mail.ru
А. Н. Медведев, email: m561@rambler.ru

Краснодарское высшее военное училище имени
генерала армии С.М. Штеменко

Аннотация. *В работе рассматриваются объекты критической информационной инфраструктуры Российской Федерации. Приводится краткий обзор методов сетевого планирования и управления, нормативной правовой базы в области защищенности значимых объектов критической информационной инфраструктуры. Предложен к рассмотрению способ проведения аудита информационной безопасности таких объектов.*

Ключевые слова: *Аудит информационной безопасности, объект критической информационной инфраструктуры, метод сетевого планирования и управления, оценка рисков информационной безопасности.*

Введение

Цель работы состоит в разработке способа проведения аудита информационной безопасности (ИБ) объектов критической информационной инфраструктуры (КИИ). Новизна работы заключается в комплексном применении известных методов сетевого планирования и управления, стандартов (методов) аудита и оценки рисков ИБ объектов КИИ и соотношения величины объёма аудита ИБ к количеству экспертов в этой области.

При построении системы обеспечения ИБ наряду с процессами реализации защитных мер, обучения персонала, внедрения политики безопасности и т. д., важное значение имеют процессы контроля и проверки состояния ИБ. Такой контроль позволяет проверить адекватность выбранных мер и средств защиты, а также выявить уязвимости в существующей информационной системе (ИС). Среди процессов контроля и проверки ИБ особое положение занимает аудит ИБ, основным назначением которого является формирование независимой оценки ИБ [1].

Основными из научно-технических проблем обеспечения информационной безопасности являются проблемы в областях:

- разработки требований и норм по защищенности критически важных ИКС России и оценки возможных рисков нарушения их безопасности;
- разработки и обоснования стратегий аудита и мониторинга безопасности инфокоммуникационных систем;
- проведения экспертиз реального уровня защищенности критически важных информационных систем в процессе их эксплуатации [2].

Предложенный способ проведения аудита ИБ позволит на практике получить численные значения уровня защищенности объектов КИИ при переходе в критичное состояние (пороговый минимум) с учетом структуры таких систем и реальных условий их функционирования.

Планирование аудита ИБ представляет собой один из важнейших этапов проверки объектов КИИ на их защищенность. От того, насколько тщательно происходит подготовка к предстоящей проверке, во многом зависит степень эффективного использования специалистов, задействованных в проверке, что закономерно обусловливает рациональное и грамотное использование их рабочего времени при одновременной экономии трудовых затрат.

Суть сетевого планирования и управления

Сетевое планирование и управление (СПУ) представляет собой систему методов, с помощью которых осуществляется планирование и управление научными и конструкторскими исследованиями и проектами, организацией и проведением крупных общественных мероприятий и т. п. Диапазон применения СПУ весьма широк: от задач, касающихся деятельности отдельных лиц, до проектов, включающих сотни организаций и десятки тысяч людей, таких как, например, создание крупного территориально-промышленного комплекса [3].

Из-за этого и возникла необходимость рассмотреть и обосновать актуальность сетевого планирования аудита ИБ с целью структурирования, детализации и возможности корректировать мероприятия по очередности, длительности и полноте при оценке защищенности объектов КИИ.

Проанализировав методы сетевого планирования, был сделан выбор в пользу «Метода критического пути (МКП) – относящегося к Детерминированному сетевому методу» и «Метода графической оценки и анализа (GERT) – относящегося к Альтернативным Вероятностным сетевым методам».

В Детерминированных сетевых методах - взаимная последовательность и продолжительности работ заданы однозначно, а Альтернативные Вероятностные сетевые методы позволяют варьировать проведением мероприятий, так как продолжительности всех или некоторых работ и связей между работами носят вероятностный характер (рис. 2).

В соответствии со Стандартом Банка России СТО БР ИББС-1.1-2007 программа аудита ИБ включает деятельность, необходимую для планирования и организации определенного количества аудитов ИБ, их контроля, анализа и совершенствования, а также обеспечения их ресурсами, необходимыми для эффективного и результативного проведения аудитов ИБ в заданные сроки.

Стандартом Банка России СТО БР ИББС-2.7-2015 определены методологические рекомендации по обеспечению необходимых и достаточных кадровых ресурсов к определению потребностей службы ИБ.

Международным стандартом ISO/IEC 27006:2015, а также Национальным стандартом РФ ГОСТ Р ИСО/МЭК 27006-2008 регламентированы процедуры определения продолжительности аудита ИБ, которые учитывают размер, характеристики, сложность и значимость потенциальных рисков ИБ, а также критерии, которые должны учитываться при определении необходимого времени аудитора.

Из поста [4] Блога Сергея Борисова, эксперта и системного интегратора в области ИБ на Кубани, виден статистический анализ и подбор нормативных правовых актов РФ и СССР в части касающейся только необходимого количества ИТ- и ИБ-специалистов в организации, опять же только для трудовой деятельности с обслуживанием объектов (АРМ, ОС, серверов, СУБД, ППО, …). На работы по ИБ или ЗИ подобных публичных норм, к сожалению, нет.

Существующее положение дел свидетельствует о том, что отсутствуют какие-либо нормативный правовые акты в мире (в т.ч. и в РФ) регламентирующие временные показатели и критерии (трудозатраты, человеко-часы) проведения конкретных мероприятий аудита ИБ, в связи с чем и требуется исследовать вариации очерёдности/длительности/полноты проведения частных работ аудита ИБ в разные промежутки времени с применением методов СПУ.

За счёт постоянного роста числа объектов КИИ требуется (в порядке доказуемости) выделение большего количества должностных лиц (экспертов) либо времени для проведения аудита ИБ, отсюда необходимо оптимизировать проведение аудита ИБ (решить оптимизационную задачу).

Состояние кибербезопасности

Проанализировав состояние ИБ в мире и РФ видно, что имеется тенденция к росту числа кибератак, в том числе и рассматриваемая модель внутреннего злоумышленника с наличием «жертвы» социальной инженерии. Причем в России наблюдаются кибератаки на объекты КИИ как из-за рубежа, так и среди своих же «хакеров».

Тем не менее защищенность объектов КИИ снижается из-за появления новых методов и способов воздействия и реализации угроз ИБ, а декомпозировав её оценку и проведение мероприятий путём введения и применения комплексных показателей (критериев) БИ на каждом этапе аудита ИБ возможно повысить качество его проведения в целом.

Руководящие документы

Анализ нормативных правовых актов РФ в области информационной безопасности (ИБ) КИИ РФ:

- раскрывает необходимость защиты КИИ и повышении её защищенности, безопасности функционирования объектов КИИ, а также достаточности сил для этих целей;
- устанавливает задачи по оценке состояния ИБ, планированию, осуществлению и оценке эффективности комплекса мер по обеспечению ИБ и организации деятельности и координации взаимодействия сил обеспечения ИБ [5].

Определены составы мер организационных и технических по обеспечению безопасности (ОБ) для значимого объекта (ЗО) соответствующей категории значимости таких как:

- регламентация правил и процедур планирования мероприятий по обеспечению защиты информации (ПЛН.0);
- разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации (ПЛН.1);
- контроль выполнения мероприятий по обеспечению защиты информации (ПЛН.2);
- регламентация правил и процедур аудита безопасности (АУД.0) [6].

Определены полномочия органам государственной власти, федеральным органам исполнительной власти и требования к ОБ ЗО КИИ, а именно:

- осуществление госконтроля, организация и проведение оценки безопасности КИИ;
- планирование, разработка, совершенствование и внедрение мероприятий по ОБ ЗО КИИ [7].

Определены следующие требования (мероприятия) по:

– планированию системы менеджмента (СМ) ИБ и оценке рисков ИБ;
– функционированию (оперативному планированию и управлению, оценке рисков ИБ и их обработке) СМИБ;
– улучшению системы менеджмента ИБ [8].

Визуальное представление способа проведения аудита ИБ

Исходя из вышесказанного разработан способ сетевого планирования аудита ИБ учитывающий пересечение следующих множеств (рис. 1):

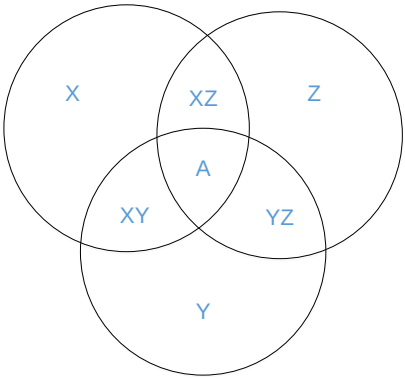

Рис. 1. Диаграмма Эйлера-Венна проведения аудита ИБ

На рисунке 1 представлены следующие обозначения:

X – Множество стандартов и методов аудита и оценки рисков ИБ [9], в которое входят элементы из таблиц 1 и 2, с применением метода Саати.

Y – Множество методов СПУ, в которое входят элементы: метод критического пути и метод графической оценки и анализа (GERT)), основанные на теории графов (рис. 2).

Z – Множество переменных отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии.

XY – подмножество зависимостей методов СПУ аудита ИБ от методов (стандартов) аудита и оценки рисков ИБ.

YZ – подмножество зависимостей методов СПУ аудита ИБ от переменных отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии.

XZ – подмножество зависимостей методов (стандартов) аудита и оценки рисков ИБ от переменных отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии.

Таблица 1

Сравнительный анализ стандартов и методов идентификации активов [9]

Стандарт / метод	Типы активов										Проводимые мероприятия						
	Информация	Бизнес-процессы	Технические средства	Программное обеспечение	Каналы и сети передачи данных	Персонал	Помещения	Организационная структура	Обеспечивающие системы	Третьи стороны	Интервьюирование	Опросные листы	Анализ документации	Физический осмотр	Анализ инцидентов	Использование инструментальных средств	Мозговой штурм
ISO/IEC серий 27000 и 31000	+	+	+	+	+	+	+	+	–	–	+	+	+	+	+	+	–
NIST SP 800 серии	+	+	+	+	+	+	–	–	–	–	+	+	+	–	+	+	–
РС БР ИББС-2.2-2009	+	+	+	+	+	–	+	–	–	–	+	+	–	–	–	–	–
Р Газпром 4.2-3-003-2015	+	+	+	+	–	–	–	–	–	–	+	+	+	+	+	+	–
MAGERIT	+	+	+	+	+	+	+	–	+	+	+	+	–	–	+	–	+
EBIOS	+	–	+	+	+	+	+	–	–	+	+	+	+	+	–	+	–
PCI DSS	+	+	+	+	+	+	–	–	–	–	+	+	–	–	+	–	–
OCTAVE	+	–	+	+	+	+	+	–	–	–	+	+	–	–	–	+	+
CRAMM	+	+	+	+	–	+	–	–	–	–	+	+	–	–	–	–	–
ГРИФ	+	+	+	+	+	+	–	+	–	–	+	+	–	–	–	–	–
RiskWatch	+	–	+	+	+	+	–	–	–	–	+	+	–	–	+	+	–
Microsoft	+	–	+	+	+	–	–	–	–	–	+	+	–	–	–	+	–

Таблица 2

Сравнительный анализ стандартов и методов анализа рисков [9]

Стандарт / метод	Виды оценки		Оценка вероятности события								Категории последствий					
			Параметры			Учитываемые факторы										
	Качественная	Количественная	Вероятность	Частота	Актуальность	Мотивация источника угроз	Возможности источника угроз	Осведомленность источника угроз	Уязвимости	Реализованные защитные меры	Прямые материальные	Косвенные материальные	Правовые	Репутационные	Ущерб жизни и здоровью	Ущерб окружающей среде
ISO/IEC серий 27000 и 31000	+	+	+	–	–	+	+	–	+	+	+	+	+	+	+	+
NIST SP 800 серии	+	+	+	–	–	+	+	–	+	+	+	+	–	+	+	–
РС БР ИББС-2.2-2009	+	+	+	–	–	+	+	–	–	+	+	+	+	+	–	–
Р Газпром 4.2-3-003-2015	+	+	+	–	–	+	+	+	+	+	+	+	+	+	+	+
BSI-Standard 100-3	+	–	–	–	+	–	–	–	–	+	–	–	–	–	–	–
MAGERIT	+	–	+	+	–	–	–	–	–	+	+	+	+	+	+	+
EBIOS	+	–	+	–	–	+	+	–	+	+	+	+	–	–	–	–
PCI DSS	+	+	+	–	–	+	+	–	+	+	+	–	–	–	–	–
OCTAVE	+	–	+	–	–	+	–	–	+	+	+	+	+	+	+	–
CRAMM	+	+	–	+	–	–	–	–	+	+	+	+	+	+	+	–
ГРИФ	+	+	+	–	–	–	–	–	+	+	+	–	–	–	–	–
RiskWatch	–	+	–	+	–	–	–	–	+	+	+	+	–	+	+	–
Microsoft	+	+	–	+	–	–	–	–	+	+	+	+	+	+	–	–

В результате получаем симбиоз конкретного стандарта (метод) аудита и оценки рисков ИБ и конкретного метода СПУ в зависимости от переменного отношения величины объёма аудита ИБ к количеству экспертов в составе комиссии, а именно:

А – как элемент достижения способа проведения аудита ИБ.

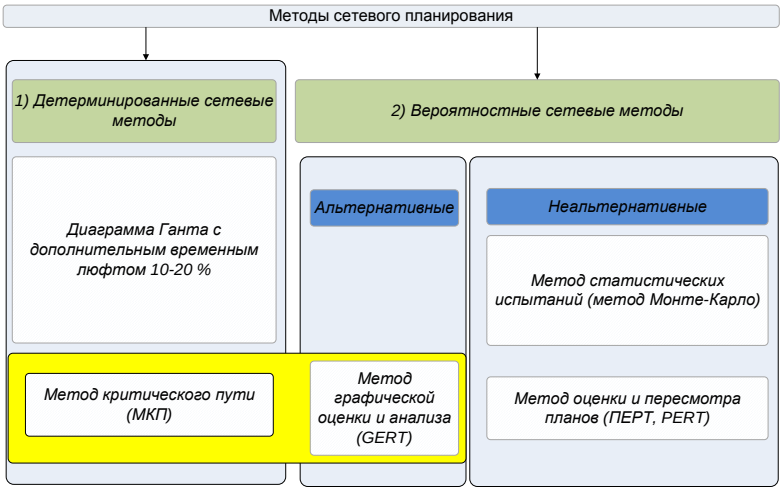

Рис. 2. Методы сетевого планирования и управления

Заключение

Возникновение новых и совершенствование существующих информационных технологий происходит постоянно и практически непрерывно (например, обновления приложений для Android выходят в Google Play в среднем раз в 28 дней), тогда как процессы совершенствования системы обеспечения информационной безопасности имеют выраженные интервалы функционирования с длительными регламентированными циклами. Справедливое желание с более высокой достоверностью осуществлять верификацию средств защиты связано с невозможностью существенно сократить эти циклы и приблизить их длительность к темпам инноваций в области информационных технологий [10].

Из всего вышесказанного следует обобщённое заключение по актуальности выдвижения указанной выше работы, а именно необходимость обоснования комплексного подхода в применении известных методов решения задач сетевого планирования аудита ИБ, оценке рисков её и достаточности сил для повышения качества, и уровня защищенности объектов КИИ за счёт:

– выбора оптимального количества должностных лиц (экспертов) в составе комиссии исходя из количества элементов объекта КИИ и состояния его защищенности;

– определения очередности (последовательно или параллельно (в т.ч. одновременно несколько)) выполнения частных мероприятий по оценке защищенности объекта КИИ; длительности (снижения/увеличения) выполнения частных мероприятий по оценке защищенности объекта КИИ; а также полноты (полностью или частично (для выдержки, выявления закономерностей)) выполнения частных мероприятий по оценке защищенности объекта КИИ;
– поддержания порогового (минимального) уровня защищенности в свете появления новых (типов, видов) угроз ИБ и способов их воздействия с применением социальной инженерии.

Список литературы

1. Макаренко, С. И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С. Макаренко // Системы управления, связи и безопасности. – 2018. – № 1. – С. 1–29.

2. Давыдов, А. Е. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем : научно-техническое издание / А. Е. Давыдов, Р. В. Максимов, О. К. Савицкий. – М. : ОАО «Воентелеком», 2015. – 520 с.

3. Плескунов, М.А. Задачи сетевого планирования : учебное пособие / М. А. Плескунов. – Екатеринбург : Изд-во Урал. ун-та, 2014. – 92 с.

4. ИТ. Норма ИТ и ИБ специалистов в гос. учреждениях [Электронный ресурс] : Блог Сергея Борисова про ИБ. Режим доступа: https://sborisov.blogspot.com/2017/11/blog-post_23.html

5. Указ Президента РФ от 5 декабря 2016 года № 646 «Об утверждении Доктрины информационной безопасности РФ» // Собрание законодательства РФ. - 12.12.2016. - № 50. - ст. 7074.

6. Приказ ФСТЭК «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. Приказа ФСТЭК России от 26.03.2019 г. №60) от 25.12.2017 г. № 239 // Российская газета. – 28.03.2018 (в ред. Российская газета. – 27.04.2019).

7. Федеральный закон РФ № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры» (в ред. Федерального закона № 193-ФЗ от 26.07.17, № 194-ФЗ от 26.07.19) // Собрание законодательства РФ. – 31.07.2017. - № 31. - ст. 4736.

8. Международный стандарт ISO/IEC 27001:2013. Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности – Требования [Текст]. –

Введ. 2013-10-01. – ISO copyright office, Case postale 56 * CP 401: CH-1211 Geneva 20, Switzerland, 2013. – с. 34

9. Лившиц, И. И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами: специальность 05.13.19 «Методы и системы защиты информации, информационная безопасность»: диссертация на соискание ученой степени доктора технических наук / Лившиц Илья Иосифович ; Санкт-Петербургский институт информатики и автоматизации Российской академии наук. – Санкт-Петербург, 2018. – 418 с. – Библиогр.: с. 109-110. – Текст : непосредственный.

10. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства [Электронный ресурс] : Общероссийский научно-практический журнал «Инновация». Режим доступа: https://maginnov.ru/ru/zhurnal/arhiv/2018/innovacii-n3-2018/innovacionnye-informacionnye-tehnologii-v-kontekste-obespecheniya-nacionalnoj-bezopasnosti-gosudarstva