УДК 004.056

Юдин Арсений Павлович, студент,
Финансовый университет при Правительстве РФ
г. Москва

Резниченко Сергей Анатольевич,
кандидат технических наук, доцент кафедры
информационной безопасности Финансового
университета при Правительстве РФ,
Финансовый университет при Правительстве РФ,
г. Москва

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КИИ: ОСОБЕННОСТИ И ТРЕБОВАНИЯ

Аннотация: В данной статье рассмотрено такое понятие, как аудит информационной безопасности, в частности аудит безопасности объектов критической информационной инфраструктуры, и проанализировано текущее законодательство в области аудита КИИ. На основе проведенного анализа были выделены основные требования и особенности проведения аудита.

Ключевые слова: информационная безопасность, аудит информационной безопасности, критическая информационная инфраструктура, законодательные требования.

С развитием законодательной базы Российской Федерации в области информационных технологий и ужесточением требований к безопасности, их соблюдение на любом предприятии становится не только желанием руководства защитить свои активы, но и краеугольным камнем существования организации как таковой. Это связано в первую очередь с наличием обязательных условий, регламентированных нормативно-правовыми документами органов исполнительной власти России: именно они определяют порядок разработки, введения и эксплуатации систем информационной безопасности, а также перечень организационно-правовых мероприятий, направленных на поддержание их эффективного функционирования.

Обеспечение безопасности объектов критической информационной инфраструктуры (далее – КИИ) – ключевая задача по обеспечению технического и информационного суверенитета РФ. В зависимости от категории значимости объекта КИИ нарушение его функционирования может привести к значимым последствиям социального, политического, экономического и/или оборонного характера и тем или иным образом повлиять на страну и жизни людей. Именно поэтому требования к защищенности объектов КИИ отличаются от общих требований и требуют более детального и скрупулёзного рассмотрения, в частности – проверки их соблюдения при проведении аудита объектов КИИ.

Рассмотрим данные понятия по порядку. Понятие КИИ закреплено законодательно, в соответствии со ст. 2 Федерального закона №187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации» критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов [1]. В свою очередь под объектами КИИ подразумеваются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры [1]. При этом объекты КИИ представляют из себя компоненты субъектов КИИ – учреждений, организаций и индивидуальных предпринимателей, функционирующих в одной из 14 основных сфер жизнедеятельности, указанных в законе. Для более понятного восприятия структуру КИИ можно представить схематично (рис. 1).

Рис. 1. Структура организации предприятий КИИ.

Процедура категорирования объектов КИИ установлена законодательно, ее регламентирует Постановление Правительства РФ №127 от 08.02.2018 г. «Об утверждении правил категорирования объектов КИИ РФ <…>», в результате которого определяется категория значимости предприятия. Алгоритм категорирования КИИ представлен следующими этапами:

1. Решением руководства создается специальная комиссия, состоящая из руководителя субъекта КИИ и уполномоченных сотрудников организации.
2. Определяются все критические процессы и подпроцессы в организации, формируется перечень объектов КИИ и их логических компонентов.
3. В соответствии с перечнем показателей критериев значимости объектов КИИ РФ, входящим в состав Постановления №127, каждому объекту КИИ организации в зависимости от значений показателей (социальная, экономическая, политическая и др. значимости) устанавливается одна из трех категорий значимости, при этом 1 категория является наивысшей.
4. По результатам категорирования каждого из объектов КИИ, предприятию устанавливается наивысшая категория значимости КИИ, ранее присвоенная одному из объектов КИИ.
5. Сведения о результатах присвоения той или иной категории направляются во ФСТЭК России не более чем через 10 дней после проведения категорирования.
6. В течение 30 дней с момента получения результатов ФСТЭК обязан проверить правильность выставления категории и внести организацию в реестр значимых объектов КИИ при подтверждении данных

Категорирование КИИ является прямым родоначальником аудита информационной безопасности, поскольку в зависимости от выставленной категории значимости варьируются требования к мерам обеспечения безопасности значимого объекта, обозначенные в Приказе ФСТЭК №239 от 25.12.2017 г. «Об утверждении требований по обеспечению безопасности значимых объектов КИИ РФ». Именно в зависимости от данных требований формируется регламент проводимого аудита. При этом важно отметить, что соблюдение данного Приказа необходимо только в том случае, если объект КИИ признан значимым, в ином случае по решению субъекта КИИ для обеспечения информационной безопасности на предприятии можно воспользоваться как Приказом №239, так и Приказом ФСТЭК от 14.03.2014 г. №31 «Об

утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах <…>», структуры требований которых схожи.

Соответственно, по результатам категорирования планируется и разрабатывается система безопасности предприятия. Однако чаще всего на момент категорирования объект КИИ уже имеет некую базовую систему защиты, поэтому до проектирования новой системы безопасности проводится так называемый диагностический аудит, в ходе которого проверяется текущее состояние защищенности информационной инфраструктуры предприятия. После его проведения определяется какие компоненты обладают достаточным уровнем защищенностью, а какие требуют обязательной доработки.

Однако единоразового формирования периметра защиты недостаточно в долгосрочной перспективе. Поскольку оборудование, программное обеспечение и организационные мероприятия безустанно устаревают, а злоумышленники и недоброжелатели каждый раз придумывают все более изощренные способы воздействия на инфраструктуру предприятия, необходимо регулярно проводить аудит информационной безопасности всех объектов КИИ.

Понятие аудита закреплено в национальном стандарте ГОСТ Р ИСО 19011–2012 «Руководящие указания по аудиту систем менеджмента»: аудит – это систематический, независимый и документируемый процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита [5]. Непосредственно аудит информационной безопасности КИИ проверяет требования, установленные после этапа категорирования предприятия КИИ и формирования полноценной системы безопасности. Во многом данные требования установлены законодательно, поэтому аудит объектов КИИ должен проводиться на регулярной основе.

Обобщая вышесказанное, под аудитом информационной безопасности понимается процесс независимой проверки состояния безопасности информационной системы, автоматизированной системы и/или организации в целом на соответствие установленным критериям, таким как: законодательные требования или внутренние регламенты и политики безопасности. Аудит является неотъемлемой частью PDCA-цикла (или же цикла Деминга) – процесса принятия решений, применимый для любой организации и используемый для управления качеством. В его состав входят следующие этапы: планирование – действие – контроль – корректировка. Именно на этапе контроля имеет место быть аудит, цель которого заключается в проверке всех установленных требований и норм, и в случае выявления отклонений или недостатков – формирование плана по краткосрочному исправлению объектов КИИ либо модернизации системы для соответствия законодательным и/или корпоративным требованиям.

Среди этапов проведения аудита информационной безопасности выделяют следующие:

1. Подготовка к аудиту. На данном этапе формируется аудиторская группа, которая представляет собой команду профессионалов, включающую в себя руководителя группы, аудиторов, ассистентов, экспертов и технических специалистов, которые принимают активное участие в проведении аудиторской проверки объектов КИИ. Подробная информация о компетенциях и требованиях к аудиторскому персоналу и органам, осуществляющим аудит, регламентирована национальным стандартом ГОСТ Р ИСО/МЭК 27006–2020.

Также на данном этапе определяются цели, границы, критерии оценки, план проведения аудита.

2. Сбор информации. Осуществляется путем первичного сбора документации и отчетов функционирования технического оборудования. А также проверки показаний сотрудников путем заполнения опросов/интервьюирования. Этот процесс позволяет проверить

достоверность информации, предоставляемой руководителями субъекта КИИ. Общение с рядовыми сотрудниками позволяет осуществить срез знаний и определить общий уровень осведомленности в области ИБ, а также узнать реальную обстановку по уровню и эффективности обеспечения информационной безопасности.

3. Анализ документации. Включает в себя проверку документов и отчетов по предыдущим проведенным аудитам, а также произошедшим событиям и инцидентам безопасности, изучение журналов активности, аутентификации пользователей и пр.

4. Анализ уязвимостей технического оборудования и программного обеспечения. Инструментальный аудит. На данном этапе проводится проверка всего оборудования и ПО, которые являются частью системы информационной безопасности на предмет соответствия установленным на этапе подготовки к аудиту критериям и отсутствия уязвимостей и угроз, зафиксированных в банке угроз и уязвимостей ФСТЭК.

Например, касаемо аудита программного обеспечения, в соответствии с недавними изменениями в российском законодательстве, согласно Указу Президента РФ от 30.03.2022 г. №166 «О мерах по обеспечению технологической независимости и безопасности КИИ РФ», а также Указу Президента №887 «о внесении изменений в Указ Президента РФ от 30.03.2022 г. №166 <…>», с 31 марта 2022 года запрещено покупать иностранные программные продукты и программно-аппаратные комплексы с целью их использования на значимых объектах КИИ. А ранее купленное иностранное ПО запрещается использовать с 1 января 2025 года.

При проведении аудита ПО необходимо учитывать данные требования; в краткие сроки необходимо согласовать новые требования к используемым на объектах КИИ программам (предпочтение отдано отечественному оборудованию и ПО).

Анализ уязвимостей объекта КИИ является обязательным этапом проведения аудита в соответствии с Приказом ФСТЭК №239. В ходе проведения анализа уязвимостей проверяется программный код прикладного ПО, конфигурации средств виртуализации, архитектуры значимого объекта, в общем говоря, он должен охватывать все программные и аппаратные средства защиты КИИ.

Один из способов проверки уровня защищенности компонентов системы безопасности является инструментальный аудит, который имитирует реальное поведение злоумышленника при атаке КИИ. Он позволяет на практике проверить эффективность существующей системы защиты в противодействии попыткам несанкционированного доступа к информационной инфраструктуре организации и информации, в ней содержащейся.

По результатам анализа уязвимостей должен быть подтвержден факт отсутствия на объекте КИИ уязвимостей, как минимум внесенных в перечень уязвимостей ФСТЭК (банк уязвимостей ФСТЭК).

5. Формирование отчета по аудиту. По результатам аудита создается отчетный документ, в котором фиксируются обнаруженные уязвимости и потенциальные угрозы безопасности, а также содержатся непосредственные требования по исправлению/улучшению системы защиты информации.

Проведение аудита информационной безопасности объектов КИИ регламентировано Приказом ФСТЭК от 21.12.2017 г. №235 «Об утверждении требований к созданию систем безопасности значимых объектов КИИ РФ <…>», в соответствии с п. 35 и 36 на регулярной основе (не реже чем раз в 3 года) должен осуществляться внутренний контроль организации работ по обеспечению безопасности КИИ, и эффективности принимаемых организационных и технических мер [8].

В ходе проведения контроля проверяется выполнение требований нормативных правовых актов в области обеспечения безопасности КИИ, а также организационно-распорядительных документов по безопасности значимых объектов КИИ.

Таким образом, по отношению к объектам КИИ в законодательном порядке установлены строгие и обязательные требования по обеспечению их защищенности. На основе данных требований и обозначенных критериев и проводится регулярный аудит информационной безопасности объектов критической информационной инфраструктуры, цель которого заключается в оценке текущего состояния защищенности системы безопасности и разработке мер по устранению ее недостатков и модернизации. Требования, описанные в статье, в первую очередь направлены на обеспечение безопасности объектов КИИ, а вследствие чего, на обеспечение технического и информационного суверенитета РФ.

Список литературы:

1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ (последняя редакция).
2. Постановление Правительства РФ от 08.02.2018 N 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»
3. Приказ ФСТЭК России от 25.12.2017 N 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
4. Приказ ФСТЭК России от 14.03.2014 N 31 (ред. от 15.03.2021) «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»
5. Национальный стандарт Российской Федерации ГОСТ Р ИСО 19011–2021 «Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента»
6. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
7. Указ Президента Российской Федерации от 22.11.2023 № 887 «О внесении изменения в Указ Президента Российской Федерации от 30 марта 2022 г. № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
8. Приказ ФСТЭК России от 21.12.2017 N 235 (ред. от 20.04.2023) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»
9. Особенности проведения аудита информационной безопасности объектов КИИ. URL: https://187.ussc.ru/news/detail/osobennosti-provedeniya-audita-informatsionnoy-bezopasnosti-obektov-kii/.
10. Что такое КИИ. URL: https://it-enigma.ru/about/news/chto-takoe-kriticheskaya-informaczionnaya-infrastruktura-%28kii%29%29.
11. Критическая информационная инфраструктура 2024 год. URL: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/.