Критическая информационная инфраструктура и безопасность её объектов.

Оглавление

Критическая информационная инфраструктура и безопасность её объектов.

1. Введение

Наука о защите информации существует и применяется уже не одну сотню лет, но почти никакие важные сведения сейчас уже не хранятся в бумажном виде и не обрабатываются в аналоговых (нецифровых) системах, поэтому и методы их защиты должны быть цифровыми. Информационные системы различных отраслей экономики все чаще становятся объектом кибератак, проводимых злоумышленниками, которые ставят своей целью похищение ценных сведений и новейших разработок, а иногда - вывод из строя атакуемых систем и даже диверсии. Поэтому принятие защитных мер стало логичной ответной реакцией.

1 января 2018 года, в нашей стране вступил в действие закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Закон).

Критическая информационная инфраструктура (сокращенно - КИИ) - это информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия.

Новый Закон предназначен для регулирования отношений в области обеспечения безопасности объектов информационной инфраструктуры РФ, функционирование которых критически важно для экономики государства.

Кроме подписания данного Закона о КИИ, были назначены федеральные органы исполнительной власти (ФОИВ), отвечающие за реализацию норм данного закона. Так, Федеральная Служба по Техническому и Экспортному Контролю (ФСТЭК) России была назначена уполномоченным ФОИВ в области обеспечения безопасности критической информационной инфраструктуры РФ. На Федеральную Службу Безопасности (ФСБ) РФ были возложены функции обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на

информационные ресурсы РФ (далее – система ГосСОПКА). Кроме этого, приказом ФСБ РФ в 2018 году был создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ), который координирует деятельность субъектов КИИ и чья техническая инфраструктура используется для функционирования системы ГосСОПКА. НКЦКИ - это Центр SOC в государственном масштабе, а система ГосСОПКА - это такая большая система SIEM для всей страны. При этом в работе системы ГосСОПКА есть особенность: информация по произошедшему компьютерному инциденту должна быть передана субъектом КИИ в систему ГосСОПКА в течение 24 часов и это удобнее делать автоматизировано, например, с помощью API системы IRP.

2. Объекты критической информационной инфраструктуры и их категории значимости.

Как отмечалось выше, Закон № 187-ФЗ от 26.07.2017 г. предназначен для регулирования отношений в области обеспечения информационной безопасности объектов, функционирование которых критически важно для экономики государства.

Такие объекты в законе называются объектами критической информационной инфраструктуры (далее – объекты КИИ). Согласно Закону, к объектам КИИ могут быть отнесены информационные системы и сети, а также автоматизированные системы управления, функционирующие в сфере:

здравоохранения;

науки;

транспорта;

связи;

энергетики;

банковской и иных сферах финансового рынка;

топливно-энергетического комплекса;

атомной энергии;

оборонной и ракетно-космической промышленности;

горнодобывающей, металлургической и химической промышленности.

Объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия между ними, составляют понятие критической информационной инфраструктуры.

Так же, как и во всех случаях защиты информации, важно определить меры по защите информации в КИИ, а для того, чтобы это осуществить, следует понять, какие объекты КИИ являются более важными и, соответственно, требуют большей защиты, а какие - не столь важны. Согласно Постановлению Правительства РФ №127 от 08.02.2018 г. категория значимости объекта КИИ может принимать одно из трех значений (где самая высокая категория - первая, самая низкая - третья) и зависит от количественных показателей значимости этого объекта в социальной, политической,

экономической и оборонной сферах. Например, если компьютерный инцидент на объекте КИИ может привести к причинению ущерба жизни и здоровью более 500 граждан, то объекту присваивается максимальная первая категория, а если услуги связи в результате инцидента КИИ могут стать недоступны для 3 тыс. - 1 млн. абонентов, то объекту присваивается минимальная третья категория. Процесс категорирования объектов КИИ проводится внутренней комиссией по категорированию субъекта КИИ, в результате чего формируется список объектов КИИ с категориями значимости и затем отправляется в ФСТЭК России, где полученные сведения вносятся в специальный реестр объектов КИИ. Таким образом, категорирование КИИ состоит из нескольких взаимосвязанных шагов, результатом которых является составление субъектом КИИ Акта категорирования КИИ и наполнение реестра объектов КИИ данными с соответствующими категориями значимости.

3. Категорирование объектов критической информационной инфраструктуры

Осуществление процедуры категорирования обязательно для всех организаций, которые являются субъектом критической информационной инфраструктуры (далее субъект КИИ) и состоит из следующих этапов:

3.1. Создание комиссии по категорированию

Возглавлять данную комиссию должен руководитель субъекта КИИ или уполномоченное им лицо. В качестве уполномоченного лица обычно выступает сотрудник, отвечающий за безопасность организации. Также в состав комиссии включаются следующие категории сотрудников субъекта КИИ:

- сотрудники, являющиеся специалистами в сфере деятельности Субъекта КИИ;
- сотрудники, осуществляющие эксплуатацию основных систем и оборудования;
- сотрудники, обеспечивающие безопасность объектов критической информационной инфраструктуры (ОКИИ);
- сотрудники подразделения по защите государственной тайны;
- сотрудники подразделения по гражданской обороне и защите от чрезвычайных ситуаций.

Действует данная комиссия на постоянной основе, то есть на весь период действия статуса «субъект КИИ». Создание комиссии по категорированию ОКИИ оформляется в виде стандартного распорядительного документа – приказа.

3.2. Выявление критических процессов субъекта КИИ

Комиссия проводит аналитическую работу по определению основных процессов в рамках осуществления видов деятельности организации – субъекта КИИ. В качестве источника информации по существующим процессам в организации могут служить устав, учредительная документация, лицензии, сертификаты, организационно-штатная структура, положения различных подразделений и прочее. На основании полученной информации, комиссии следует выявить среди всех процессов только те, которые являются критическими.

3.3. Составление перечня ОКИИ

Комиссия осуществляет инвентаризацию инфраструктуры своей организации с целью выявления информационных систем (далее ИС), автоматизированных систем управления (далее АСУ) или информационно-телекоммуникационных сетей (далее ИТКС), которые обеспечивают выполнение критических процессов субъекта КИИ.

3.4. Направление во ФСТЭК России перечня ОКИИ

Комиссия оформляет полученный перечень ОКИИ, подлежащих категорированию в соответствии с рекомендуемой ФСТЭК России формой (см. Информационное сообщение ФСТЭК России от 24 августа 2018 г. N 240/25/3752), которая утверждается руководителем субъекта КИИ или уполномоченным лицом, а также регулятором сферы деятельности субъекта КИИ. Утвержденную форму на бумажном и электронном носителе необходимо направить на согласование во ФСТЭК России.

3.5. Присвоение категории значимости ОКИИ

Далее у субъекта возникает обязательство: в течение одного года с момента утвержденного перечня ОКИИ осуществить процедуру присвоения категории значимости ОКИИ.

ОКИИ классифицируются на значимые и не значимые. В свою очередь, если объект является значимым, то ему может быть присвоена первая, вторая или третья категория. В зависимости от присвоенной категории значимости изменяется состав обязательных организационных и технических мер обеспечения безопасности ОКИИ. В случае, если ОКИИ не относится к значимым, для него не применяются дополнительные составы мер обеспечения безопасности, которые приведены в подзаконных актах Федерального закона № 187.

В рамках процедуры категорирования комиссия субъекта КИИ:

- выполняет моделирование действий нарушителей и рассматривает иные источники угроз безопасности информации в отношении ОКИИ,
- производит анализ угроз безопасности информации и уязвимостей, которые могут привести к возникновению компьютерных инцидентов на ОКИИ.

Далее комиссия по категорированию производит оценку возможных последствий в результате возникновения компьютерных инцидентов каждого ОКИИ на основании 14-ти показателей значимости ОКИИ РФ и их значений, которые приведены в Постановлении Правительства РФ № 127. Важно отметить, что категория значимости ОКИИ присваивается по максимальному значению одного из критерия значимости.

Результирующим документом данного процесса является утвержденный комиссией субъекта КИИ акт категорирования ОКИИ с присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Содержание данного документа базируется на форме из Приказа ФСТЭК России от 22 декабря 2017 г. N 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

3.6. Направление во ФСТЭК России результата присвоения категории ОКИИ

На последнем этапе комиссии по категорированию необходимо в течение 10-ти дней со дня утверждения актов категорирования ОКИИ направить результаты в ФСТЭК России по форме Приказа ФСТЭК России от 22 декабря 2017 г. N 236.

4. Защита информации в критических информационных инфраструктурах

Защита КИИ – особенно важный процесс информационной безопасности.

Объективные факторы, влияющие на кибербезопасность промышленных предприятий:

- эволюция технологических процессов;
- изменение процессов управления производством;
- постоянно возрастающая техническая сложность систем управления технологическим процессом;
- уменьшение времени жизни систем управления;
- повышение степени автоматизации, избавление от ручного труда;
- укрупнение производств, покупки и слияния;
- увеличение уровня защищённости «традиционных» жертв киберпреступников;
- отсутствие очевидной повседневной угрозы — функциональной (технологическому процессу, оборудованию) и физической (людям и окружающей среде) безопасности, бизнесу промышленных организаций;
- неохотное раскрытие информации об уязвимостях, атаках и инцидентах;
- геополитика.

Проблемы кибербезопасности промышленных предприятий:

- постоянно растущее количество и разнообразие уязвимостей и угроз;
- постоянно увеличивающийся интерес к промышленным организациям киберкриминала и спецслужб;
- недооценка общего уровня угрозы;
- неправильное понимание специфики угрозы и неоптимальный выбор средств защиты;
- технические и организационные сложности защиты АСУ ТП.

Кроме уже указанных выше документов, ФСТЭК России выпустил ряд нормативных документов, которые детально описывают процесс защиты

информации в КИИ. Например, один из основных документов - это Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». Его требуется применять тогда, когда организация-субъект КИИ провела процедуру категорирования своих объектов КИИ и пришла к выводу, что среди них есть значимые объекты критической информационной инфраструктуры (сокращенно - ЗОКИИ).

Приказ №239 говорит, что разработка мер защиты информации значимого объекта КИИ должна включать в себя анализ угроз безопасности и разработку модели угроз безопасности КИИ:

1. **Анализ угроз** включает в себя выявление источников угроз, оценку возможностей нарушителей (т.е. создание модели нарушителя), анализ уязвимостей используемых систем, определение возможных способов реализации угроз и их последствий. Модель нарушителя строится на основе предположений о потенциале атакующих, т.е. о мере усилий, затрачиваемых нарушителем при реализации угроз безопасности информации в информационной системе (при этом потенциалы нарушителей можно условно разделить на высокий, средний и низкий).

Анализ уязвимостей можно произвести при помощи тестов на проникновение - пентестов (англ. PenTest, сокращение от Penetration Test). При проведении пентестов проверяющие определяют слабые места инфраструктуры компании, выявляют уязвимости в системах защиты, проводят контролируемую эмуляцию настоящей хакерской атаки - в общем, наглядно показывают, что компания - заказчик этого тестирования может быть взломана. Далее заказчик получает рекомендации по устранению выявленных в ходе пентеста недочетов, и через какое-то время пентест повторяется. При проведении анализа уязвимостей и способов реализации угроз рекомендуется использовать Банк Данных Угроз (сокращенно – БДУ) ФСТЭК России - это официальный государственный справочник различных уязвимостей и способов атак, который регулярно пополняется и поддерживается в актуальном состоянии.

2. Под **построением модели угроз** безопасности КИИ при защите КИИ подразумевается описание свойств или характеристик угроз безопасности информации, а под угрозой безопасности - совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (т.е. базовых свойств информации, о которых мы уже говорили). Целью моделирования угроз КИИ является нахождение всех условий и факторов, проводящих к нарушению безопасности информации и работы ИТ-систем. Модель угроз может строиться на основе следующего классического подхода: актуальная угроза информационной безопасности возникает при наличии источника угрозы (внешний/внутренний нарушитель или третьи силы), уязвимости актива, способа реализации угрозы, объекта воздействия и самого вредоносного воздействия. Кроме того, совсем недавно ФСТЭК России выпустил проект новой методики моделирования угроз безопасности информации, которую можно применять для моделирования угроз в критической информационной инфраструктуре. В соответствии с данной Методикой, угроза безопасности информации является актуальной, если существует источник угрозы, условия и сценарий для её реализации, а воздействие на активы приведет к негативным последствиям. В Методике сказано, что процесс моделирования угроз ИБ состоит из следующих этапов:

- определение возможных негативных последствий от реализации угроз по результатам оценки рисков нарушения законодательства, бизнес-процессов и/или нарушения защищенности информации, что может привести к таким негативным последствиям, как нарушение законодательства, экономический или репутационный ущерб;

- определение условий для реализации угроз безопасности информации, т.е. выявление уязвимостей, недекларированных возможностей, доступов к ИТ-системам, которые могут быть использованы злоумышленниками;

- определение источников угроз (техногенных и антропогенных) и оценка возможностей нарушителей (внешних и внутренних);

- определение сценариев реализации угроз с помощью таблицы тактик и техник атакующих, приведенной в Методике;

- оценка уровня опасности угроз безопасности информации путем анализа типа доступа, необходимого для реализации атаки, сложности сценария атаки и уровня важности атакуемых активов.

После анализа и моделирования угроз следует переходить к внедрению контрмер. При этом внедряемые меры защиты не должны оказывать негативного влияния на функционирование самого объекта КИИ – этим подчеркивается, что приоритетом является непрерывность технологических процессов, остановка которых может сама по себе привести к инциденту на КИИ, например, к выходу оборудования из строя или даже аварии.

В списке организационных и технических мер, предусмотренных положениями данного приказа № 239 в зависимости от категории значимости объекта КИИ и угроз безопасности информации, указаны следующие пункты:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;
- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- планирование мероприятий по обеспечению безопасности;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- реагирование на инциденты информационной безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

Кроме этого, в Приказе №239 особо оговорено, что при использовании СЗИ для защиты КИИ приоритет отдается штатному защитному функционалу, а при реагировании на компьютерные инциденты в критической информационной инфраструктуре требуется отправлять информацию о них в систему ГосСОПКА. Указывается также на важность использования СЗИ, которые обеспечиваются гарантийной и/или технической поддержкой, а также на возможные ограничения по использованию программного/аппаратного обеспечения или СЗИ (видимо, имеются ввиду санкционные риски). Также указано, что на значимом объекте КИИ требуется запретить удаленный и локальный бесконтрольный доступ для обновления или управления лицами, не являющимися работниками субъекта КИИ, а также запретить бесконтрольную передачу информации из объекта КИИ производителю или иным лицам. Кроме этого, все программные и аппаратные средства объекта КИИ первой категории значимости должны располагаться на территории РФ (за исключением оговоренных законодательством случаев).

Приказ №239 применяется в случае, если объект КИИ признан значимым (т.е. ему присвоена одна из трех категорий значимости). Если же объект КИИ признан незначимым (т.е. ни одна из категорий значимости не была присвоена), то по решению субъекта КИИ можно применять как Приказ №239 по КИИ, так и Приказ ФСТЭК России от 14 марта 2014 г. № 31 «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». Данный Приказ №31 посвящен защите АСУТП - автоматизированных систем управления производственными и технологическими процессами, а положения данного Приказа близки к нормам Приказа №239.

Для автоматизации процессов категорирования и обеспечения безопасности объектов критической информационной инфраструктуры разрабатывается и используется различное программное обеспечение, например, программный комплекс **Security Vision КИИ.** Security Vision КИИ позволяет учесть все важные детали и профессионально обеспечить соответствие

законодательству, избежав временных и финансовых затрат, которых требует прохождение многочисленных и трудоемких процедур.

С его помощью в автоматическом режиме реализуются хранение и учёт объектов КИИ на протяжении всего их жизненного цикла, а также формирование отчётности и другие процедуры, предусмотренные законодательными и нормативными документами в области защиты КИИ.

Внедрение Security Vision КИИ обеспечивает полное соответствие требованиям 187-ФЗ с актуализацией в реальном режиме времени. Иными словами, Security Vision КИИ – это навигатор, который проводит организацию через все процедуры, предусмотренные законом, и обеспечивает полное и своевременное соблюдение регуляторных норм. Важной особенностью Security Vision КИИ являются его гибкость и адаптируемость - комплекс создан на базе графического конструктора рабочих процессов, который дает Заказчику возможность настроить базовые процедуры защиты КИИ в соответствии со своими уникальными внутренними бизнес-процессами.

Security Vision КИИ позволяет субъектам КИИ:

- собирать и структурировать всю информацию по объектам КИИ на единой платформе – провести инвентаризацию, анализ угроз и уязвимостей, построить модели угроз и нарушителя
- категорировать объекты КИИ согласно законодательству
- осуществлять непрерывный контроль соответствия защищенности объектов КИИ нормативным требованиям в условиях меняющегося ИТ ландшафта
- корректировать отклонение настроек систем и средств защиты от заданных параметров
- визуализировать оперативную информацию на графической панели – дашборде
- автоматизировать формирование отчетности по форме регулятора.
- накапливать статистику и базу знаний по вопросам соблюдения Федерального закона
- реализовать автоматизированное взаимодействие с НКЦКИ (ГосСОПКА) с помощью API-интеграции.

5. Заключение

Защита КИИ - критической информационной инфраструктуры - представляет из себя сложную, но интересную задачу. Это достаточно новое направление в информационной безопасности. Как было сказано выше, для реагирования на инциденты ИБ в КИИ создана система ГосСОПКА - государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. В систему ГосСОПКА следует отправлять данные из средств защиты и обработки инцидентов ИБ в КИИ, причем осуществлять это целесообразнее всего с применением автоматизированных средств, таких как системы SIEM и IRP с модулем API-интеграции с ГосСОПКА. Субъектам КИИ необходимо подключаться к ведомственным или корпоративным Центрам ГосСОПКА, либо создавать свои Центры ГосСОПКА, но это требует существенных затрат. Для защиты информации в КИИ требуется выполнять комплекс организационных и технических мер по обеспечению безопасности информации в КИИ, перечисленных в том числе в Приказах №239 и №31 ФСТЭК России.

Защита КИИ – особенно важный процесс информационной безопасности, учитывая ответственность за несоблюдение положений законодательства, объем нормативных актов и сжатые сроки реагирования на инциденты.

Вместе с утверждением ФЗ «О безопасности КИИ» в УК РФ была добавлена новая статья 274.1, которая устанавливает уголовную ответственность должностных лиц субъекта КИИ за несоблюдение установленных правил эксплуатации технических средств объекта КИИ или нарушение порядка доступа к ним вплоть до лишения свободы сроком на 6 лет. В случае наступления последствий от невыполнения необходимых мероприятий по обеспечению безопасности объекта КИИ (аварий и чрезвычайных ситуаций, повлекших за собой крупный ущерб) непринятие таких мер подпадает по состав 293 статьи УК РФ «Халатность». Дополнительно прорабатываются изменения в административное законодательство в части определения штрафных санкций для юридических лиц за неисполнение Закона. С большой долей уверенности можно говорить о том, что именно введение существенных денежных штрафов будет стимулировать субъекты КИИ к выполнению требований Закона.

6. Список литературы

1. Закон № 187-ФЗ от 26.07.2017 г. «О безопасности критической информационной инфраструктуры Российской Федерации»

2. Постановлению Правительства РФ №127 от 08.02.2018 г. «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. Информационное сообщение ФСТЭК России N 240/25/3752 от 24.08.2018 г.

4. Приказа ФСТЭК России N 236 от 22.12.2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»

5. Приказ ФСТЭК России № 239 от 25.12.2017 г. «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

6. Приказ ФСТЭК России от 14 марта 2014 г. № 31 «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».

7. **https://www.securityvision.ru/blog/kii-chto-eto/**

8. **https://www.securityvision.ru/blog/kategorirovanie-obektov-kriticheskoy-informatsionnoy-infrastruktury-v-ramkakh-187-fz-chast-1-postano/**

9. **https://www.securityvision.ru/products/kii/**

10. **https://ics-cert.kaspersky.ru/reports/2018/02/06/zakon-o-bezopasnosti-kii-v-voprosakh-i-otvetah/**

11. **https://ics-cert.kaspersky.ru/reports/2018/12/05/challenges-of-industrial-cybersecurity/**