УДК 004.056

Гильманова Э.А.
Магистрант ФГБОУ «КГЭУ»
г. Казань, Россия
Ахметшина Р.И.
Магистрант ФГБОУ ВО «КГЭУ»
г. Казань, Россия
Научный руководитель:
Исмагилов И.Р.
кандидат технических наук, доцент, ФГБОУ «КГЭУ»
г. Казань, Россия.

ОСОБЕННОСТИ ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ В ТОПЛИВНО-ЭНЕРГЕТИЧЕСКОМ КОМПЛЕКСЕ

Аннотация

В статье рассматриваются особенности проведения аудита информационной безопасности объектов критической информационной инфраструктуры в топливно-энергетическом комплексе. Обозначены цели защиты информации, выявлены виды объектов критической информационной инфраструктуры. Предложены рекомендации по проведению аудита ИБ с учетом особенностей систем промышленной автоматизации.

Ключевые слова

Защита информации, аудит, категорирование, информационная безопасность, информационные ресурсы, топливно-энергетический комплекс.

Gilmanova E.A.
Master's student of FGBOU «KGEU»
Kazan, Russia
Akhmetshina R.I.
Master's student of FGBOU VO «KGEU»
Kazan, Russia
Scientific supervisor:
Ismagilov I.R.
Candidate of Technical Sciences, Associate Professor, FGBOU VO «KGEU»
Kazan, Russia.

FEATURES OF THE INFORMATION SECURITY AUDIT OF CRITICAL INFORMATION INFRASTRUCTURE FACILITIES IN THE FUEL AND ENERGY COMPLEX

Annotation

The article discusses the specifics of conducting an audit of information security of critical information infrastructure facilities in the fuel and energy complex. The objectives of information protection are outlined, the types of objects of critical information infrastructure are identified. Recommendations for conducting an audit of information security, taking into account the features of industrial automation systems, are proposed.

Keywords

Information protection, audit, categorization, information security, information resources, fuel and energy complex.

В последнее время происходит переход индустриального информационного общества к глобальному в рамках развитых стран. В настоящий момент информация – важная составляющая экономики, как материальные или энергические ресурсы.

Важным критерием информации является ее доступность. Обычно полная ее доступность обеспечивается комплексом мероприятий по информационной безопасности (ИБ).

Цели защиты информации применительно к объектам КИИ в топливно-энергетическом комплексе:

– обеспечение доступности информации и непрерывного функционирования компонентов систем и сетей, необходимых для обслуживания критических бизнес-процессов, (например, передача и распределение электрической энергии, генерация электрической энергии, диспетчерское управление энергосистемой);

– предотвращение несанкционированного доступа к охраняемым данным, их разглашения и утечки;

– устранение противоправных действий по уничтожению, модификации, искажению, копированию, блокированию технологической информации

– предотвращение иных форм незаконного вмешательства в информационные системы, обеспечение правового режима документированной информации как объекта собственности;

– защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

– сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством.

Обеспечение безопасности информации в корпоративных системах представляется более менее ясной процедурой. А что происходит в сфере промышленного производства? Что отличает объекты ТЭК от реального сектора? Как правило, полным отсутствием комплементарности информационных атрибутов, а также и не совсем четким пониманием важности обрабатываемой на этих объектах информации.

Типовой объект автоматизации в энергетическом секторе обладает развернутой вычислительной сетью, подключением к центральному объекту. Прямое подключение к сети Интернет объекта автоматизации в данном случае сопряжено с большими рисками информационной безопасности, поэтому в топологии вычислительной сети такого предприятия выделяют три зоны:

– корпоративная — отвечает за процессы жизнедеятельности предприятия и сотрудников, — АСУП;

– исполнительная — обеспечивает выполнение технологических процессов (ТП) организации, — АСУ ТП;

– зона диспетчеризации — влияет на ход выполнения ТП [3, с.3-6].

Системы промышленной автоматизации очень отличаются корпоративных систем тем, что первые – системы реального времени, работают с быстро изменяющимися процессами, занимаются сбором и обработкой больших объемов данных, которые поступают от многочисленных датчиков на технических объектах и выдают управляющее воздействие на исполнительные механизмы. Корпоративные - выполняют комплексный учет и автоматизацию бизнес-процессов, работают с данными, которые поступают от человека. Эти данные копятся в больших объемах, но скорость их появления в системе не является критичной [4, с.45-48].

Особенность аудита ИБ систем промышленной автоматизации заключается в том, что проведение инструментального аудита (выявление уязвимостей сканерами безопасности, тестирование на проникновение – пентест) нужно осуществлять с особой осторожностью, не допустив негативного влияния на технологический процесс. А в случае, если такие действия осуществляются, то их следует проводить в период технического обслуживания, что в свою очередь, накладывает ограничения по времени проведения аудита [1, с.269]. Кроме того, аудиторам необходимо иметь специализированные программные и программно-аппаратные средства для анализа содержимого данных, передаваемых по различным промышленным протоколам и интерфейсам, для выявления аномалий, способных блокировать или модифицировать критичную технологическую информацию. Немаловажная часть аудита ИБ в ТЭК – проверка корректности настроек встроенных средств защиты информации прикладного программного обеспечения, через которое осуществляется управление и мониторинг технологического процесса. ПО современных SCADA-систем предлагает богатый функционал по защите информации. Эффективное использование данного функционала позволит значительно снизить расходы на внедрение наложенных средств защиты информации, тем самым сократить бюджет на обеспечение мероприятий по информационной безопасности. Таким образом, перед

проведением аудита необходимо ознакомиться с возможностями прикладного ПО, используемого в программно-технических комплексах автоматизации предприятия, заблаговременно направить запрос вендорам ПО о наличии данных возможностей и проанализировать полученную информацию.

Во время процесса аудита ИБ объектов КИИ нужно обратить внимание на два вида объектов КИИ:

– значимые – объекты КИИ, которые получили свою категорию значимости во время категорирования;

– незначимые – объекты КИИ, у которых отсутствует надобность наличия категории, либо объекты КИИ, которые не принимают участие в автоматизации критических процессов и, тем самым, не подлежащие категорированию.

Понимание классификации объектов КИИ нужно для определения критериев аудита ИБ. Иными словами, если в границы аудита попадают незначимые объекты КИИ, во время оценки аудитор способен не учитывать выполнение требований нормативно-правовых актов по обеспечению безопасности значимых объектов КИИ, но должен дать оценку, насколько полно выполняются субъектом КИИ обязанности, возложенные на него ч. 2 ст. 9 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [2, с.32-35].

По решению субъекта КИИ для обеспечения безопасности незначимого объекта КИИ также может быть создана система безопасности, которая базируется на требованиях для значимых объектов КИИ. В этом случае в критерии аудита уже включаются все требования, характерные для безопасности значимых объектов КИИ.

Необходимость проведения аудита ИБ значимых объектов КИИ законодательно предусмотрена в виде внутреннего аудита, проводимого работниками субъекта КИИ, либо внешнего аудита, проводимого специализированной организацией [5, с.10-11].

В заключение отметим, что описанные методический подход, система мероприятий по обеспечению безопасности информации технологических

сегментов АСУ ТП и комплекс средств защиты могут служить основой для технического проекта конкретной системы и типизированных решений.

Рекомендуется проработать техники применения РД ФСТЭК РФ в части обработки информации ограниченного доступа, более широко развить политики ИБ и распределение ответственности за защищаемые информационные ресурсы.

Список использованной литературы

1. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков. 3-е изд., стереотип. М.: ФЛИНТА, 2016. 269 с.

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Рос. газета. № 167. 31.07.2017. С.32-35

3.LETA – IT Company. Аудит ИБ [Электронный ресурс]. URL: http://www.leta.ru/services/information-security-management/audit informationsecurity.html (Дата обращения 10.12.2021 г.);

4. Филимонова Е.В. Информатика и информационные технологии в профессиональной деятельности. – М.: Юстиция, 2019. С.45-48.

5. АйТи. Система ИБ. Аудит ИБ [Электронный ресурс]. URL: http://www.it.ru/services/sub/sud_detail.php?ID=383&SUB_ID=6916 (Дата обращения 04.01.2022 г.)