Мироненко Ярослав

Информационная безопасность ИСУ

Ключевые нормативные документы

1. Федеральный закон о т 26.07.2017 N2 187-Ф3 «О безопасности критической информационной инфраструктуры Российской Федерации»
2. Федеральный закон от 27.07.2006 N2 149-Ф3 «Об информации, информационных технологиях и о защите информации»;
3. Федеральный закон от 27.07.2006 N2 152-Ф3 «О персональных данных»;
4. Приказ ФСТЭК России о т 25.12.2017 N2 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
5. «Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры», утвержденная Заместителем директора ФСТЭК России 18.05.2007;
6. «Базовая модель угроз безопасности персональных данных при обработке в информационной системе персональных данных», утвержденная Заместителем директора ФСТЭК России 15.02.2008
7. Приказ Минцифры от 30.12.2020 № 788 «Об утверждении перечня и спецификации защищенных протоколов передачи данных, которые могут быть использованы для организации информационного обмена между компонентами интеллектуальной системы учета электрической энергии (мощности) и приборами учета электрической энергии, которые могут быть присоединены к такой системе»

Критическая информационная инфраструктура

Критическая информационная инфраструктура (далее КИИ) — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ, а также сети электросвязи, используемые для организации их взаимодействия. Категорирование КИИ проводится в соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ и постановления Правительства РФ 08.02.2018 № 127.

Интеллектуальная система учета – это всегда КИИ.

В соответствии с Постановление Правительства РФ от 19 июня 2020 г. N 890:
9. В интеллектуальной системе учета для пользователей интеллектуальной системы учета должны быть реализованы следующие функции:
…
в) полное и (или) частичное ограничение режима потребления электрической энергии (приостановление или ограничение предоставления коммунальной услуги), а также возобновление подачи электрической энергии …

Категория ИСУ определяется в зависимости от показателей ущерба: Причинение ущерба жизни и здоровью людей (человек), Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений и т.п.

В случае нарушения работы ИСУ может быть прервано электроснабжение нефтеперерабатывающего завода, а также субабонентов – сетей связи, транспортной инфраструктуры и т.д.

Например, при рассмотрении показателей экологической значимости: при вредном воздействии на окружающую среду за пределами территории одного субъекта Российской Федерации или территории города федерального значения, ИСУ присваивается **первая категория значимости**. Расстояние от Московского Нефтеперерабатывающего Завода до деревни Беседы Московской области – менее 3 км.

Базовая и частная модель угроз

Владельцы ИСУЭ, которым на праве собственности, аренды или ином законном основании принадлежат объекты критической информационной инфраструктуры, обязаны определять угрозы безопасности информации

Базовая модель угроз

1. Определена Министерством энергетики Российской Федерации совместно с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации (письмо от 29.06.2021 г. No НШ-7491/07
2. Содержит перечень угроз достаточный для применения к объектам ЖКХ и гражданской промышленности
3. Не содержит информации о вариантах нейтрализации рассматриваемых угроз
4. Ориентирована на типовые проектные решения ИСУ, в большей степени относящиеся к бытовому сектору
5. Должна быть пересмотрена до 31.12.2023 г.

Частная модель угроз

1. Определяется собственником ИСУ
2. Включает угрозы, применимые в отношении конкретного рассматриваемого объекта
3. Формируется во-многом исходя из возможных вариантов нейтрализации угроз из базового перечня
4. Ориентирована на конкретное проектное решение
5. Должна пересматриваться при изменении законодательства, появлении новых угроз, изменения структуры ИСУ
6. Включает СКЗИ

Меры обеспечения безопасности

Состав необходимых мер для категорированных КИИ утвержден приказом ФСТЭК России от 25 декабря 2017 г. № 239, для КИИ без категории – локальными нормативными актами предприятия.

Меры обеспечения безопасности значимого объекта

1. Идентификация и аутентификация (ИАФ)
2. Управление доступом
3. Ограничение программной среды *(только 1-2 категория)*
4. Защита машинных носителей информации
5. Аудит безопасности
6. Антивирусная защита
7. Предотвращение вторжений (компьютерных атак) *(только 1-2 категория)*
8. Обеспечение целостности
9. Обеспечение доступности
10. Защита технических средств и систем
11. Защита информационной (автоматизированной) системы и ее компонентов
12. Реагирование на компьютерные инциденты
13. Управление конфигурацией
14. Управление обновлениями программного обеспечения
15. Планирование мероприятий по обеспечению безопасности
16. Обеспечение действий в нештатных ситуациях
17. Информирование и обучение персонала

Практически реализуемые методы

1. Установление контролируемой зоны.
2. Контроль физического доступа к объекту.
3. Планирование обеспечения непрерывности работы.
4. Идентификация и аутентификация.
5. Средства антивирусной защиты.
6. Межсетевое экранирование (периметр сети).
7. Средства резервного копирования и резервирования.
8. Разграничение прав доступа.
9. Использование сертифицированного ПО
10. Использование сертифицированного оборудования
11. Использование сертифицированных облачных сервисов

Определение мер обеспечения безопасности необходимо проводить на основе модели угроз и возможных последствий компьютерных инцидентов

Персональные данные в ИСУ

Постановление Правительства РФ от 19 июня 2020 г. N 890 «О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)»

б) сведения о пользователях интеллектуальной системы учета по соответствующей точке поставки (точке учета):
для юридических лиц - полное наименование, номер записи в Едином государственном реестре юридических лиц и дата ее внесения в реестр;
для индивидуальных предпринимателей - номер записи в Едином государственном реестре индивидуальных предпринимателей и дата ее внесения в реестр;
адрес энергопринимающего устройства;
***номер договора энергоснабжения (лицевого счета физического лица)**, договора, содержащего положения о предоставлении коммунальной услуги по электроснабжению (лицевого счета физического лица), договора купли-продажи (поставки) электрической энергии (мощности), договора оказания услуг по передаче электрической энергии;*

В соответствии с Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ данная информация становится персональными данными, если добавить ФИО.

Обеспечение защиты персональных данных

Защита персональных данных обеспечивается в соответствии с Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ.

Оператор персональных данных должен:
1. Обеспечить их защиту в зависимости от типа персональных данных и типа угроз
2. Зарегистрироваться в качестве оператора персональных данных в Роскомнадзоре
3. Получить согласие на сбор и обработку персональных данных

Тип персональных данных

Специальные (расовая и национальная принадлежность, политические, религиозные и философские взгляды, состояние здоровья, подробности интимной жизни, информация о судимостях), биометрические (фотографии, отпечатки пальцев, группа крови), общедоступные (ФИО, место регистрации, информация о месте работы, номер телефона, email) или иные (зарплата, периоды отпусков, стаж).
Отношений с субъектами персональных данных: собственные сотрудники или люди, не связанные с организацией трудовыми отношениями.
Количества субъектов персональных данных: больше 100 000 или меньше 100 000.

Тип угрозы

Определяется в соответствии с "Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" (утв. ФСТЭК РФ 14.02.2008)
Можно определить при наличии сертификата ФСТЭК для используемого программного обеспечения, либо провести экспертизу.

1 тип — самые серьезные угрозы, связанные с недокументированными возможностями в системном программном обеспечении (ПО), например в операционной системе.
2 тип — угрозы, связанные с недокументированными возможностями в прикладном ПО, например в установленных программах.
3 тип — угрозы, не связанные с ПО, например уязвимости в оборудовании.

Уровни защищенности персональных данных

Обеспечивается в соответствии с Приказ ФСТЭК от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
Определяется в соответствии с Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	до 100 тыс.			более 100 тыс.	до 100 тыс.		более 100 тыс.	до 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Уровни защищенности персональных данных

Всего существует 4 уровня защищенности (доверия):

4 УЗ – наиболее распространенный, необходим для защиты общедоступных и иных данных с 3 типом угроз. Самый простой, требует несложных мер защиты вроде установки антивируса и регулярного обновления ПО.

3 УЗ кроме общедоступных и иных данных позволяет хранить биометрические и специальные данные, работать при 2 и 3 типе угроз. Требует регулярно искать и устранять уязвимости в оборудовании и ПО, а также ограничить доступ к настройкам информационной системы. Именно этот уровень подходит для большинства компаний.

2 УЗ подходит для хранения любых данных, для некоторых данных допускает даже 1 тип угроз. Требует установить систему обнаружения вторжений, защищать систему от спама, организовать резервное копирование.

1 УЗ позволяет хранить специальные и биометрические данные при 1 типе угроз. Технически самый сложный, к примеру, требует безотказной работы серверов и установки на компьютеры только ПО, заранее разрешенного службой безопасности.

Меры по обеспечению безопасности для 4-го уровня защищенности

1. Идентификация и аутентификация субъектов доступа и объектов доступа
2. Управление доступом субъектов, в т.ч. реализация защищенного удаленного доступа, регламентация и контроль использования в информационной системе технологий беспроводного доступа и мобильных технических средств
3. Определение состава и содержания информации, сбор, запись и хранение информации о выбранных событиях безопасности
4. Антивирусная защита
5. Контроль установки обновлений программного обеспечения
6. Контроль и управление физическим доступом к техническим средствам
7. Обеспечение защиты персональных данных при передаче по каналам связи, имеющим выход за пределы контролируемой зоны

Постановление Правительства РФ от 19 июня 2020 г. N 890 "О порядке предоставления доступа к минимальному набору функций интеллектуальных систем учета электрической энергии (мощности)"

39. Необходимость шифрования (применение средств криптографической защиты) информации при ее передаче по каналам связи интеллектуальной системы учета определяется субъектами электроэнергетики, являющимися владельцами интеллектуальных систем учета, самостоятельно.
При определении ... необходимости шифрования ... рекомендуется руководствоваться базовой моделью нарушителя (моделью угроз безопасности информации)…

Базовая модель угроз безопасности информации интеллектуальной системы учета электрической энергии

Угрозы, которые могут быть нейтрализованы только с помощью средств криптографической защиты информации, сертифицированных ФСБ России, определяются для каждого конкретного информационно-вычислительного комплекса в зависимости от наличия объектов критической информационной инфраструктуры, подключаемых к ней, а также от необходимости обработки информации, подлежащей защите в соответствии с законодательством Российской Федерации

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности

Использование СКЗИ для обеспечения безопасности персональных данных необходимо в следующих случаях:
- если персональные данные подлежат криптографической защите в соответствии с законодательством Российской Федерации;
- если в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью СКЗИ
К случаям, когда угрозы могут быть нейтрализованы только с помощью СКЗИ, относятся:
- *передача персональных данных по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при 6 передаче персональных данных по информационно-телекоммуникационным сетям общего пользования) ...*

СПАСИБО ЗА ВНИМАНИЕ!

Мироненко Ярослав
Заместитель генерального директора АО «РЭС Групп»
Индивидуальный член РНК СИГРЭ
Россия, 600017, Владимир, ул. Сакко и Ванцетти, д. 23 оф.9
Тел. 8(4922) 22-21-62 доб. 702,
Моб. 8 (910) 090-11-48
mironenko@orem.su