УДК 04.056

КОМПЛЕКСНАЯ ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ НА ПРИМЕРЕ ЕНЕРГОСБЫТОВОЙ КОМПАНИИ

Старченко А. В., студент гр. ИБс-211, V курс

Научный руководитель: Прокопенко Е.В., к.ф.-м.н., заведующий кафедрой
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

Энергосбытовая компания – не просто торговая структура, а объект критической инфраструктуры, крупный участник рынка ПДн. Подобное положение относится и к информационным системам предприятия: они работают с персональными данными множества клиентов, с данными коммерческого учета электроэнергии, от которых зависят финансовые расчеты на оптовом рынке. Закон требует, чтобы компания гарантировала сохранность всех этих данных — без искажений и утечек. Важно учитывать два круга требований: общие по защите персональных данных (№152-ФЗ, 21 приказ ФСТЭК) и специальные — по безопасности КИИ (использование сертифицированных СЗИ, подключение к ГосСОПКА и т. д.).

Злоумышленники идут по многоэтапной схеме — формальное соблюдение требований уже не спасает. Если компания не будет соответствовать реальным угрозам, ей грозит не только потеря денег и доверия клиентов, но и штрафы от регуляторов и, в худшем случае — компания может столкнуться с остановкой деятельности, поскольку это объект КИИ.

Поэтому в работе предлагается не просто констатировать, что уязвимости есть, а провести комплексную оценку защищенности – с описанием угроз, рисков и предписаниями по устранению выявленных недостатков. Только так можно улучшить реальную информационную безопасность организации.

Критерии:

- Анализ требований нормативных документов и архитектуры ИС
- Моделирование угроз и профилирование злоумышленника.
- Аудит конфигураций.
- Разработка рекомендаций по совершенствованию СЗИ на основе анализа рисков.

Актуальность темы

На энергосбытовые компании в настоящее время оказывают давление два закона. Первый (152-ФЗ «О персональных данных») предусматривает, что компания должна защитить персональные данные огромного количества людей, то есть самый высокий уровень защищённости с жёсткими требованиями контролирующих органов. По второму (187-ФЗ «О безопасности КИИ») - АИИС КУЭ и биллинговые системы являются критической информационной инфраструктурой, в связи с чем возникает необходимость в категорировании объектов КИИ, использовании сертифицированных СЗИ, подключение к

ГосСОПКА. Кроме этого, в 2025 году вступили в силу изменения в ФЗ-58, ужесточающие ответственность за инциденты на объектах КИИ.

Проникновение злоумышленников в АИИС КУЭ и искажение показаний приборов учёта приведёт к неправильным расчётам с оптовым рынком и большим убыткам. В случае, если шифровальщик поразит биллинговую систему, то счёт и получение платежей полностью остановятся. Если базы данных потребителей "утекут", компания будет ждать большие штрафы и потеря репутации. Это не теория, а вполне реальный сценарий, который уже был у других компаний.

Обычные антивирусы и межсетевые экраны не являются достаточно эффективными. Злоумышленники в наше время прибегают к социальной инженерии, находят и используют уязвимости в местах стыков между системами и в веб-приложениях. Еще достаточно весомая часть угроз идет от "инсайдеров" - сотрудников, которые имеют доступ к системам и могут навредить, иногда даже не намеренно. Борьба с этим арсеналом угроз возможна только в комплексе, зная все уязвимые места.

Задачи исследования:

– Изучить архитектуру информационных систем компании.
– Выявить, как хранятся и передаются обрабатываемые данные.
– Ознакомиться с требованиями безопасности, применимыми к компании.
– Определить, каким из них существующая система защиты должна соответствовать.
– Разработать модель угроз и модель нарушителя.
– Провести аудит конфигураций, сканирование уязвимостей и выполнять сетевой анализ.
– Определить последовательность исправления уязвимостей оценить риски.
– Разработать практические решения по оптимизации средств защиты и оценить их эффективность.

Фундамент для анализа

Анализ нормативной базы показал, что рассматриваемая организация подпадает под требования двух регулирующих сфер. Игнорировать какой-то из них нельзя, так как проверяющие органы разные, а штрафы суммируются.

Первый контур отражает защиту персональных данных по 152-ФЗ. По сути, это «чек-лист», по которому можно проверить, всё ли сделано правильно. Бизнес использует личные данные многих клиентов, включая имена паспорта адреса истории оплат и т.д. Это падает под классификацию специализированных персональных данных, а количество субъектов кратно превышает 100 тысяч человек. По постановлению №1119 это автоматически означает УЗ-1 (самый высокий уровень защищённости). Кроме того, приказ ФСТЭК №21 предписывает, какие конкретные меры безопасности должны быть реализованы от многофакторной аутентификации до сертифицированных средств криптографии.

Второй контур - безопасность КИИ по 187-ФЗ. Система коммерческого учёта электроэнергии и биллинговая система должны быть категорированы, поскольку энергосбытовая компания является субъектом КИИ. От стабильности её работы зависит энергоснабжение потребителей и функционирование рынка электроэнергии. Для них нужно:

Определить категорию значимости по методике ФСТЭК
– Использовать только сертифицированные СЗИ

– Подключиться к государственной системе обнаружения компьютерных атак
– Обеспечить регистрацию событий безопасности и их анализ

При этом в 2025 году вступили в силу поправки ФЗ-58, усиливающие ответственность за нарушения на объектах КИИ. Теперь штрафы для физ. лиц достигают сотен тысяч рублей, а для компаний - миллионов. Также, регуляторы теперь обладают большими полномочиями по контролю и реагированию на инциденты.

Важно: эти два контура не существуют изолированно. АИИС КУЭ может одновременно быть и объектом КИИ, и обрабатывать ПДн. При таком варианте требования накладываются друг поверх друга, и защита должна строиться по высшему стандарту.

Угрозы, актуальные для обычной компании, здесь тоже работают, но к ним добавляются ещё и отраслевые.

Внешние угрозы.

Главные игроки - киберпреступники, которые хотят денег. Они способны зашифровать биллинговую систему и потребовать за это выкуп (классический пример «ransomware»). Базы персональных данных могут быть украдены и проданы, например, в «даркнете». Также, подвергнуться атаке может сайт или личный кабинет – сбой системы обслуживания клиентов. Но есть и более серьёзные угрозы: хакерские группы, поддерживаемые на государственном уровне. Такие команды охотятся за доступом к объектам КИИ. Для них энергосбыт - это точка входа в энергосистему региона, и их атаки могут быть частью более масштабных кампаний.

Внутренние угрозы.

Этот вид угроз часто недооценивают, но инсайдеры зачастую даже опаснее внешних хакеров. Администраторы БД, операторы биллинговой системы, сотрудники техподдержки и т.д. Все эти люди имеют легитимный доступ к системам и данным. Если такой сотрудник решит продать базу ПДн или подкорректировать показания счётчика конкретному человеку за вознаграждение - это может оставаться незамеченным долгое время. А уволенные/уволившиеся по собственному желанию сотрудники, у которых вовремя не отозвали доступ - классическая проблема многих компаний.

Ещё одна проблема - сложность инфраструктуры. В компании множество систем, которые обмениваются данными через общие базы данных, файловые обменники и т.п. Каждый такой стык - потенциальная уязвимость в общей системе, через которую можно пройти во всю сеть.

Комплексная оценка защищённости.

Многие считают, что оценка защищённости - это банальный запуск сканера и получение списка уязвимостей. На самом деле - это системный процесс, который включает в себя несколько этапов:

Моделирование угроз по методике ФСТЭК.

Прежде чем что-то сканировать, нам нужно понять, что именно мы защищаем и от кого. Для этого описываются общие границы системы и выделяются ценные активы (ПДн, данные АИИС КУЭ, файлы конфигурации), определяются возможные нарушители и шаблоны их действий. На выходе мы получаем модель угроз - документ, который в дальнейшем используется для настройки СЗИ и проведения тестов.

Инструментальный анализ.

Сканирование уязвимостей, пентест (тестирование на проникновение), анализ веб-приложений и их кода. Важно, что пентест должен имитировать реальные действия нарушителя из модели угроз, а не просто перебирать всё подряд. Для энергосбыта особенно важно тестировать сегменты АИИС КУЭ и биллинга, но делать это так, чтобы не нарушить рабочие процессы.

Аудит конфигураций и организационных мер.

Проверка соответствия настройки операционных систем и межсетевых экранов требованиям безопасности. Например, приказ ФСТЭК №21 требует, чтобы пароли были сложными, велись журналы событий (аудит), а доступ к данным разграничивался. Часто оказывается, что формально требования выполнены, но на практике пароли наклеены под клавиатурами, а журналы никто не просматривает.

Анализ рисков.

На этом этапе все выявленные проблемы расставляются по степени опасности. Уязвимость, которая может позволить хакеру получить доступ из интернета напрямую к базе ПДн - это критический риск, который необходимо устранять в первую очередь.

Разработка рекомендаций.

На основе анализа рисков формируется план мероприятий: что делать и в какие сроки, какие СЗИ стоит закупать.

Только пройдя все эти этапы, можно говорить о действительно комплексной оценке.

СПИСОК ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных...».
4. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры».
5. Методика оценки угроз безопасности информации (утв. ФСТЭК России 05.02.2021).

Стандарты

1. ГОСТ Р ИСО/МЭК 27001-2021 «Системы менеджмента информационной безопасности. Требования».
2. ГОСТ Р 59533-2021 «Защита информации. Обеспечение безопасности объектов критической информационной инфраструктуры. Общие положения».
3. ГОСТ Р МЭК 62443-2-1-2020 «Сети промышленной автоматизации. Безопасность промышленных систем».

Основная литература

1. Лукин А.В., Курило А.П. Безопасность критических инфраструктур. - М.: Горячая линия – Телеком, 2022.
2. Белов Е.Б., Лоскутов А.А. Моделирование угроз безопасности информации. - М.: Горячая линия – Телеком, 2022.
3. Иванов М.А., Козлов Д.А. Проблемы обеспечения безопасности АИИС КУЭ как объектов КИИ // Вопросы кибербезопасности. - 2024. - № 2.