Обзор изменений законодательства в сфере информационной безопасности 2019-2021

Андрей Березов

Руководитель департамента информационной безопасности

ООО «Информационный центр»

(423) 240-48-66 доб. 7201

and@ic-dv.ru

ЦБ РФ, 17 апреля 2019 года

Обязательные требования по защите информации:

683-П – для **кредитных** организаций;

684-П – для **некредитных** организаций;

Оба документа предписывают использовать:

ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;

ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

Оба документа в полной мере не вступили в силу.

Кто такие некредитные организации?

Согласно статье 76.1 Федерального закона № 86-ФЗ «О ЦБ РФ»:

- профессиональные участники рынка ценных бумаг;
- управляющие компании фондов;
- организации, занимающиеся клиринговой деятельностью;
- центральные контрагенты;
- организаторы торговли;
- центральные депозитарии;
- репозитарии;
- страховые компании;
- негосударственные пенсионные фонды;
- микрофинансовые организации;
- кредитные потребительские кооперативы;

Кто такие некредитные организации?

Согласно статье 76.1 Федерального закона № 86-ФЗ «О ЦБ РФ»:

- жилищные накопительные кооперативы;
- бюро кредитных историй;
- организации, занимающиеся актуарной деятельностью;
- кредитные рейтинговые агентства;
- сельскохозяйственные кредитные потребительские кооперативы;
- операторы инвестиционной платформы;
- ломбарды;
- операторы финансовой платформы;
- операторы ИС, в которых осуществляется выпуск цифровых активов;
- операторы обмена цифровых финансовых активов.

Приказ ФСТЭК от 20.02.2020 № 35

«О внесении изменений…» в приказ ФСТЭК № 239

Новые требования к СЗИ и к прикладному ПО (вступают в силу с 1 января 2023 года).

Запрет удаленного доступа к ЗОКИИ, при невыполнении обязательных требований по защите и мониторингу удаленного доступа.

Приказ министерства здравоохранения московской области от 20.08.2020 №1123

«Об утверждении методических рекомендаций по определению объектов критической информационной инфраструктуры на объектах информатизации медицинских организаций для учреждений государственной системы здравоохранения Московской области»

Является неплохим методически документом по определению и категорированию объектов КИИ для **всех** учреждений здравоохранения.

ФСТЭК России. Февраль 2021 г. Проект методического документа

«Рекомендации по оценке показателей критериев экономической значимости объектов критической информационной инфраструктуры Российской Федерации»

Используется при категорировании объектов КИИ.

Информационное сообщение ФСТЭК России от 15.10.2020 г. №240/24/4268

«Об утверждении требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий»

До 1 января 2021 г. все СЗИ должны быть пересертифицированы с требований по НДВ на требования по уровням доверия.

Федеральный закон от 30.12.2020 №515-ФЗ

«О внесении изменений в отдельные законодательные акты Российской Федерации в части обеспечения конфиденциальности сведений о защищаемых лицах и об осуществлении оперативно-розыскной деятельности»

Вносит изменения в пункт 6 части 2 статьи 19 Федерального закона «О персональных данных»:

- *2. Обеспечение безопасности персональных данных достигается, в частности:*
- *6) обнаружением фактов несанкционированного доступа к персональным данным и принятием мер,* ***в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них***;

Наш разбор ситуации: https://habr.com/ru/company/ic-dv/blog/538012 /

Федеральный закон от 26.05.2021 №141-ФЗ

«О внесении изменений в Кодекс Российской Федерации об административных правонарушениях»

Вводит административные штрафы за нарушение законодательства в области КИИ:

Нарушение	Физ. лица, тыс. руб.	Юр. лица, тыс. руб.	Статья КоАП
Нарушение требований к созданию систем безопасности ЗОКИИ (вступает в силу с 01.09.2021 г.)	10-50	50-100	13.12.1 (1)
Нарушение порядка информирования о компьютерных инцидентах	10-50	100-500	13.12.1 (2)
Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами КИИ	20-50	100-500	13.12.1 (3)
Непредоставление (или нарушение сроков) во ФСТЭК данных о категорировании	10-50	50-100	19.7.15 (1)
Непредоставление (или нарушение сроков) передачи информации в ГосСОПКу	10-50	100-500	19.7.15 (2)

Методический документ. Методика оценки угроз безопасности информации

Утвержден ФСТЭК России 5 февраля 2021 г.

Положительные моменты:

- методика применяется для моделирования угроз всех типов объектов информатизации (ИСПДн, ГИС, АСУ ТП, ЗОКИИ, иные АС и ИС);
- не рассматриваются вопросы, связанные с техническими каналами;
- методика направлена на оценку антропогенных угроз (при этом рассматривать техногенные угрозы никто не запрещает);
- применяется в ИС, решение о создании/модернизации которых принято позже 05.02.2021 (есть некоторый переходный период);
- есть рекомендуемая структура документа;
- явно разрешено делать МУ для предполагаемой архитектуры;
- явно разрешено поддерживать МУ в актуальном состоянии в электронном виде.

Методический документ. Методика оценки угроз безопасности информации

Утвержден ФСТЭК России 5 февраля 2021 г.

Важный момент:

При размещении ИС в стороннем ЦОД, в случае, если владелец ЦОД не провел оценку угроз, необходимо исходить из предположения, что ЦОД скомпрометирован.

Таким образом, ГИС, размещаемая в ЦОД, владелец которого отказывается предоставлять документы по оценке актуальных угроз не сможет быть аттестована.

Методический документ. Методика оценки угроз безопасности информации

Требует вдумчивого подхода:

- слишком много сущностей, нередко дублирующих друг друга;
- основной текст методики, рекомендуемая структура и приложения-примеры зачастую противоречат друг другу;
- тактики и техники нарушителей ориентированы только на внешнего злоумышленника, таким образом выпадают возможные сценарии связанные со случайными неквалифицированными действиями и/или прямым физическим доступом;
- помимо понятия «актуальные угрозы», вводится понятие «возможные угрозы». Чтобы из списка возможных угроз получить список актуальных угроз необходимо составить сценарии реализации угроз из тактик и техник и проверить применимость этих сценариев к возможным угрозам. Этот этап является очень трудоемким и по факту бессмысленным, так как оба списка всегда совпадают.

Методический документ. Методика оценки угроз безопасности информации

Отрицательные моменты:

Документ предписывает пользоваться БДУ ФСТЭК, но сама БДУ не переделана под терминологию методики.

$УБИ_i$ = [нарушитель (источник угрозы); объекты воздействия; способы реализации угроз; негативные последствия].

В БДУ три уровня потенциала, в методике четыре. Понятия «внешний» и «внутренний» нарушитель концептуально противоположные

В БДУ не описаны

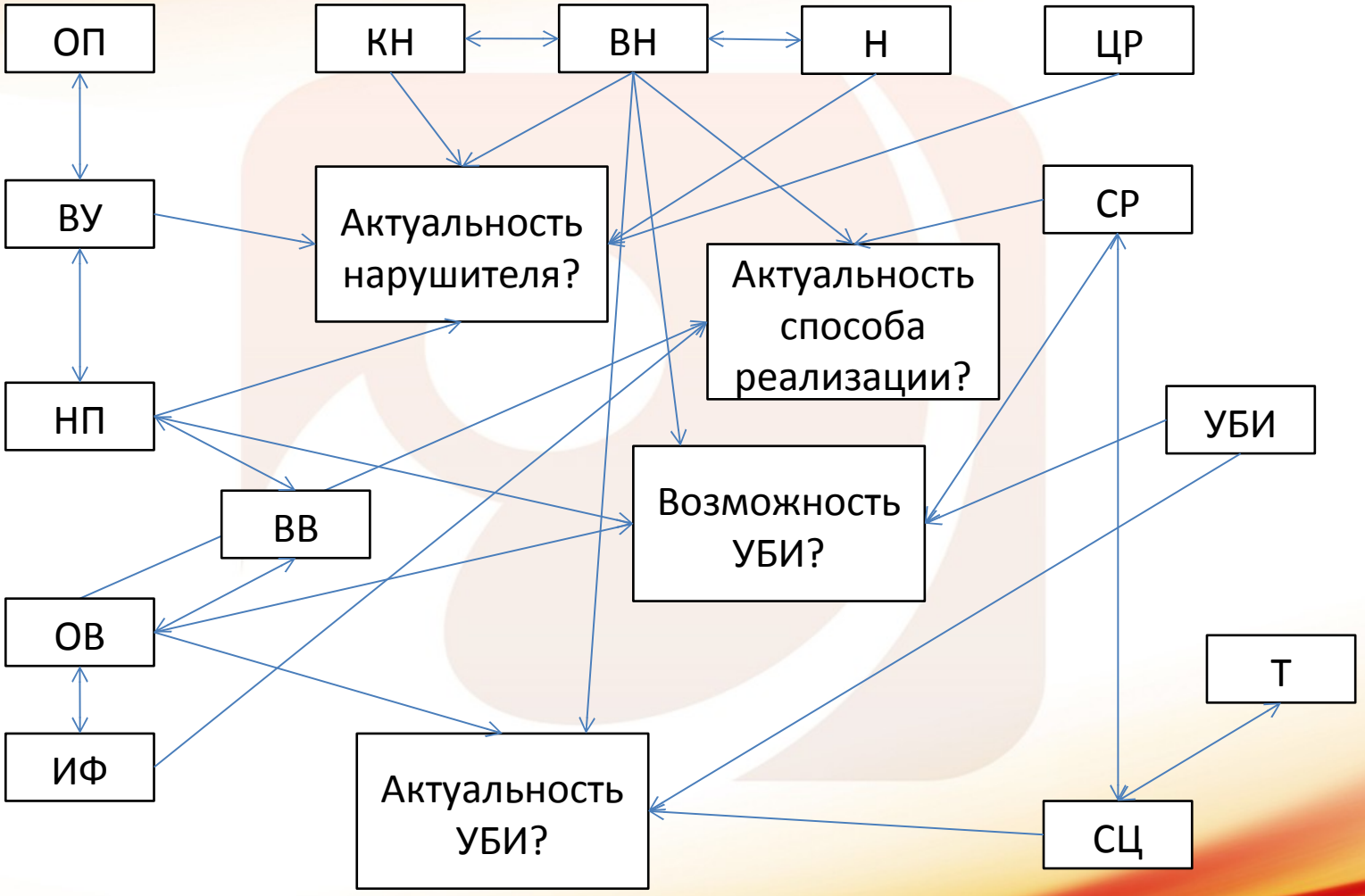
В БДУ привязаны к нарушению К, Ц, Д, но в методике применяется расширенное толкование

Стоит отметить, что ФСТЭК знает об этой проблеме и работает над адаптацией БДУ к новой методике МУ

Сущности, которыми необходимо оперировать специалисту при разработке МУ

- основные процессы, для обеспечения которых создается ИС (ОП);
- виды риска (ущерба) (ВУ);
- возможные негативные последствия (НП);
- объекты воздействия на аппаратном, системном, прикладном уровнях, уровне сетевой модели взаимодействия, уровне пользователей (ОВ);
- виды воздействия (ВВ);
- категория нарушителей (КН);
- виды нарушителей (ВН);
- уровень возможностей нарушителей (Н);
- возможные цели реализации угрозы безопасности (ЦР);
- способ реализации угрозы безопасности (СР);
- доступные нарушителю интерфейсы воздействия (ИФ);
- угроза безопасности информации (УБИ);
- тактики и техники реализации угроз безопасности (Т);
- сценарии реализации угроз безопасности (СЦ).

Необходимо определить сами сущности (многие вручную) и их взаимосвязи



ФСТЭК обещает в ближайшем будущем некое средство автоматизации моделирования угроз

Пример несогласованности основного текста, рекомендуемой структуры и приложений

п. 4.6:Объекты воздействия определяются на **аппаратном, системном и прикладном уровнях**, на **уровне сетевой модели взаимодействия**, а также на **уровне пользователей**.

Пример – Приложение 5.

Приложение 5
к Методике оценки угроз
безопасности информации

Примеры определения объектов воздействия и видов воздействия на них

Таблица 5.1

Негативные последствия	Объекты воздействия	Виды воздействия
Разглашение персональных данных граждан (У1)	База данных информационной системы, содержащая идентификационную информацию граждан	Утечка идентификационной информации граждан из базы данных
	Удаленное автоматизированное рабочее место (АРМ) пользователя	Утечка идентификационной информации граждан с АРМ пользователя
	Линия связи между сервером основного центра обработки данных и сервером резервного центра обработки данных	Перехват информации, содержащей идентификационную информацию граждан, передаваемой по линиям связи
	Веб-приложение информационной системы, обрабатывающей идентификационную информацию граждан	Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы

Разбивка по уровням в примере – отсутствует.

Структура неоптимальная и нелогичная, объекты воздействия должны быть в крайнем левом столбце.

Согласно рекомендуемой структуре МУ перечень объектов воздействия это один раздел, а их связь с видами воздействия и негативными последствиями – другой.
В примере все в одной таблице.

Хотелось бы определенности…

5.1.7. Внешние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых. Внутренние нарушители реализуют угрозы безопасности информации преднамеренно (преднамеренные угрозы безопасности информации) с использованием программных, программно-аппаратных средств или без использования таковых или непреднамеренно (непреднамеренные угрозы безопасности информации) без использования программных, программно-аппаратных средств.

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ

Резюме по методике МУ

- в целом много положительных моментов – учтены современные технологии, отдельно оговорены границы ответственности заказчика и провайдера облачных услуг в различных ситуациях;
- в целом разработка и сам документ стали сложнее и запутаннее, особенно без средств автоматизации;
- многие этапы проводятся экспертным методом, таким образом качество документа напрямую зависит от качества эксперта;
- ждем от ФСТЭК обновления БДУ, самой методики и средство автоматизации.

Благодарю за внимание!

Андрей Березов

Руководитель департамента информационной безопасности

ООО «Информационный центр»

(423) 240-48-66 доб. 7201

E-mail: and@ic-dv.ru