Модель угроз безопасности информации НФО как составная часть интегрированной СУР и роль ИИ в её создании

Конференция ПАРТАД «Инфраструктура рынка ценных бумаг и искусственный интеллект – 2025»
11 июля 2025 года, г. Калуга

Нормативная база
для оценки и моделирования угроз безопасности информации

- Положение Банка России от 15 ноября 2021 г. № 779-П "Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76^1 Федерального закона от 10 июля 2002 года № 86-ФЗ "О Центральном банке Российской Федерации (Банке России)", в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)»
- Приказ ФСТЭК от 11 февраля 2013 г. № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"
- Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"
- Методика оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.)

Положение Банка России от 15 ноября 2021 г. № 779-П

Некредитные финансовые организации, обязанные соблюдать **усиленный, стандартный или минимальный** уровень защиты информации, в рамках обеспечения операционной надежности **должны**:

- **моделировать информационные угрозы** в отношении критичной архитектуры;
- планировать применение организационных и технических мер, направленных на реализацию требований к операционной надежности, на основе результатов оценки риска реализации информационных угроз в рамках системы управления рисками (при наличии);
- обеспечивать реализацию требований к операционной надежности на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации своих объектов информационной инфраструктуры;
- обеспечивать контроль соблюдения требований к операционной надежности в отношении элементов критичной архитектуры.

Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17

Формирование требований к защите информации, содержащейся в информационной системе, в том числе включает:

- **определение угроз безопасности информации**, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе **модели угроз безопасности информации**.

В качестве **исходных данных** для определения угроз безопасности информации используется **банк данных угроз безопасности информации** (bdu.fstec.ru), ведение которого осуществляется ФСТЭК России, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются **методические документы**, разработанные и утвержденные ФСТЭК России.

По решению обладателя информации (заказчика) или оператора настоящие Требования могут применяться для защиты информации, содержащейся в **негосударственных** информационных системах.

Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239

Разработка организационных и технических мер по обеспечению безопасности значимого объекта **должна включать**:

- **анализ угроз безопасности информации** и **разработку модели угроз безопасности информации** или ее уточнение (при её наличии).

В качестве **исходных данных** для анализа угроз безопасности информации используется **банк данных угроз безопасности информации**, ведение которого осуществляется ФСТЭК России, а также источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации **должны** применяться **методические документы**, разработанные и утвержденные ФСТЭК России.

По решению субъекта критической информационной инфраструктуры настоящие Требования **могут** применяться для обеспечения безопасности объектов **критической информационной инфраструктуры**, **не отнесенных к значимым объектам**.

Методика ФСТЭК оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.)

Методика применяется для определения **угроз безопасности информации**, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, **значимым объектам критической информационной инфраструктуры** Российской Федерации.

В **иных случаях** решение о применении настоящей Методики принимается обладателями информации или операторами систем и сетей.

По результатам оценки **угроз безопасности информации**, проведенной в соответствии с настоящей Методикой, **должны** быть выявлены **актуальные угрозы безопасности информации**, реализация (возникновение) которых может привести к нарушению безопасности обрабатываемой в системах и сетях информации и (или) к нарушению, прекращению функционирования систем и сетей.

Методика ФСТЭК оценки угроз безопасности информации (утв. ФСТЭК России 5 февраля 2021 г.)

Оценка угроз безопасности информации включает следующие **этапы**:

1) **определение негативных последствий**, которые могут наступить от реализации (возникновения) угроз безопасности информации (финансовые, производственные, репутационные или иные виды рисков (ущерба));

2) **определение возможных объектов воздействия** угроз безопасности информации (информационные ресурсы и компоненты систем и сетей, виды воздействия на них);

3) **оценка возможности реализации** (возникновения) угроз безопасности информации:

- **определение источников** угроз безопасности информации (виды и категории актуальных нарушителей)
- **оценка способов реализации** (возникновения) угроз безопасности информации (актуальные способы реализации угроз и типы интерфейсов объектов воздействия, сценарии (тактики и техники) реализации угроз)

4) **оценка актуальности** угроз безопасности информации:

УБИi = [**нарушитель** (источник угрозы); **объекты воздействия**; **способы реализации угроз**; **негативные последствия**]

Модель интегрированной системы управления рисками (ИСУР)

Модель угроз безопасности информации НФО как один из элементов интегрированной системы управления рисками (ИСУР)

Модель УБИ – **прогнозная** составляющая ИСУР в части управления рисками ИБ (поддерживается в актуальном состоянии, осуществляется мониторинг угроз безопасности информации и оценка эффективности имеющихся защитных мер).

В случае реализации (фактического наступления) угроз безопасности информации (в т.ч. вследствие отсутствия или недостаточности (неэффективности) защитных мер) данное событие **фиксируется** в БДР как реализация операционного риска (подвид риск ИБ) и включается в общую статистику и отчетность по управлению рисками.

Для интеграции с ИСУР модель УБИ должна включать **меры защиты информации** (ГОСТ Р 57580.1-2017) в привязке к актуальным угрозам безопасности информации, а также содержать ссылку на запись в БДР в случае реализации УБИ.

Модель угроз безопасности информации – прогнозная составляющая ИСУР в части управления рисками ИБ

Выявление актуальных угроз безопасности информации (прогноз)

Реализация угрозы (фактическое наступление негативного события ИБ)

Формат записи базы данных модели угроз безопасности информации

(1) Объекты защиты	(2) Объекты воздействия		(3) Виды воздействия	(4) Источники угроз безопасности информации					(5) Способы реализации (возникновения) УБИ		(6) Негативные последствия от реализации УБИ		(7) УБИ	(8) Сценарии реализации УБИ		(9) Меры защиты информации (ГОСТ Р 57580.1-2017)			(10) Реализация угроз безопасности информации (фиксация события в БДР)				
Наименование систем и сетей, для которых разработана модель угроз безопасности информации	Группы информационных ресурсов и компонентов систем и сетей, которые могут являться объектами воздействия	Типы интерфейсов объектов воздействия	Виды воздействия на информационные ресурсы и компоненты систем и сетей	Виды нарушителей (антропогенные источники угроз безопасности информации)	Цели реализации угроз безопасности информации	Уровни возможностей нарушителей	Категории нарушителей в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования этих систем и сетей, а также от установленных возможностей нарушителей	Техногенные источники угроз безопасности информации	Основные способы реализации (возникновения) угроз безопасности информации	Идентификатор уязвимости (База данных уязвимостей ФСТЭК)	Виды риска (ущерба)	Возможные типовые негативные последствия	Идентификатор УБИ (База данных угроз ФСТЭК)	Основные тактики	Основные техники	Условное обозначение и номер меры	Организационная мера	Техническая мера	Дата и время выявления (обнаружения) реализации угрозы	Дата и время реализации угрозы	Причина реализации угрозы	Фактические негативные последствия (ущерб)	Номер записи в БДР

Объективные трудности, связанные с разработкой и внедрением модели угроз безопасности информации в НФО

- ✓ Значительный объём **внутренней информации** (объекты воздействия и виды воздействия на них, виды и категории внутренних нарушителей, способы реализации угроз и типы интерфейсов объектов воздействия, сценарии реализации УБИ, тактики и техники внутренних нарушителей)

- ✓ Значительный объём **внешней информации** (виды и категории внешних нарушителей, техногенные источники УБИ, виды уязвимостей и угроз безопасности информации и иная информация из банка данных угроз безопасности информации ФСТЭК России)

- ✓ Значительный объём **рутинной и аналитической работы** специалистов НФО по обработке всего объёма внутренней и внешней информации для выявления актуальных для организации угроз безопасности информации

Возможности применения искусственного интеллекта (ИИ) при создании модели угроз безопасности информации

- ✓ **Машинная обработка** всей имеющейся в организации внутренней и внешней информации, являющейся исходными данными для создания модели УБИ

- ✓ **Выявление угроз безопасности информации**, являющихся актуальными для организации, **поддержание модели УБИ в актуальном состоянии** (в случае изменения внутренней или внешней исходной для модели информации)

- ✓ **Значительное сокращение трудовых и временных затрат** организации, связанных с определением актуальных угроз безопасности информации и поддержанием актуальности модели УБИ

Благодарю за внимание!

Бекаревич Павел Викторович
Независимый эксперт по управлению рисками
Генеральный директор ООО «ПБекар-РМ»
pbekar@rambler.ru