AKTIV.CONSULTING

Требования регулятора. Где спрятаны расходы?

Фаина Митрофанова

Независимый эксперт
по информационной безопасности

Взаимосвязь стандартов

Комплекс национальных стандартов «Безопасность финансовых (банковских) операций»

Структура комплекса стандартов		
Семейство стандартов УР	Управление риском реализации информационных угроз и обеспечения операционной надежности	ГОСТ 57580.3
	Методика оценки зрелости	**В разработке**
Семейство стандартов ОН	Обеспечение ОН	ГОСТ 57580.4
	Методика оценки соответствия	**В разработке**
Семейство стандартов ЗИ	Защита информации ФО	ГОСТ 57580.1
	Методика оценки соответствия	ГОСТ 57580.2

В настоящее время обязательным стандартом является только ГОСТ 57580.1, т.к. для него разработана методика оценки.
Методики оценки соответствия для ГОСТ 57580.3 и ГОСТ 57580.4 находятся в разработке, публикация ожидается в 1Q 2024 г.

ГОСТ 57580.3

	Процесс	Требования	Следствие
1	**Организация ресурсного (кадрового и финансового) обеспечения**	**ОРО.5.1.** Установление требований на основе профессиональных стандартов к квалификации работников, в том числе профессионального стандарта для специалистов по ИБ в кредитно-финансовой сфере	**Сотрудники ИБ (включая заместителя руководителя, курирующего функцию) должны иметь профильное образование или профессиональную переподготовку**
		ОРО.6. Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния кадровых рисков в рамках деятельности по управлению риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, учитывающих в том числе: • Возможность ухода работников, задействованных при выполнении ключевых ролей по управлению риском реализации информационных угроз, обеспечению операционной надежности и защиты информации; • Возможность возникновения конфликта интересов при выполнении ролей по управлению риском реализации информационных угроз, обеспечению операционной надежности и защиты информации	**Неизбежное расширение штата ИБ (для снижения риска конфликта интересов необходимо минимум 3 сотрудника: ответственный за выполнение технических функций, риск-координатор и ответственный за соблюдение требований ИБ)**
		ОРО.17. Организация целевого обучения работников, задействованных в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, в частности организация целевого обучения по вопросам противостояния реализации информационных угроз для администраторов	**План регулярного повышения квалификации сотрудников ИБ**
		ОРО.18. Включение в разрабатываемые программы целевого обучения по вопросам выявления и противостояния реализации информационных угроз: • практических занятий, в рамках которых отрабатываются вопросы выявления индикаторов раннего обнаружения реализации информационных угроз *(индикаторов (факторов) компрометации объектов информатизации)* и реагирования на них; • Практических занятий, в рамках которых отрабатываются вопросы противостояния реализации информационных угроз на основе возможных сценариев реализации информационных угроз; • Практических занятий, в рамках которых отрабатываются вопросы восстановления после реализации инцидентов, связанных с реализацией информационных угроз, в том числе сбора и анализа технических данных *(свидетельств)*	**Киберучения сотрудников ИБ и ИТ (чтобы кого-то учить, нужно сначала собрать эффективную команду)**

ГОСТ 57580.3

	Процесс	Требования	Следствие
2	**Контроль системы управления риском реализации информационных угроз**	**УПК.2.** Установление и реализация программы проведения независимой профессиональной оценки зрелости процессов планирования, реализации, контроля и совершенствования систем управления, определенных в рамках семейств стандартов ОН и ЗИ Комплекса стандартов, согласно соответствующим методикам оценки соответствия *(далее – аудиты ОН и ЗИ)*	**Проведение внешнего аудита (аналогично ГОСТ 57580.1)**
		УПК.3. Установление плана самооценки ОН и ЗИ для каждого проводимого аудита, определяющего: • цель самооценки ОН и ЗИ • критерии самооценки ОН и ЗИ • область самооценки ОН и ЗИ • дату и продолжительность проведения самооценки ОН и ЗИ • состав аудиторской группы • описание деятельности и мероприятий по проведению самооценки ОН и ЗИ • распределение ресурсов при проведении самооценки ОН и ЗИ	**Проведение самооценки для ИТ и ИБ**
3	**Выявление событий риска реализации ИУ**	**ВСР.3.6.** Хранение в базе событий информации о выявленных событиях риска реализации информационных угроз, в том числе сведений о проведении их анализа не менее пяти лет	**Меры требуют технической реализации (т.е. подразумевают внедрение АС)** **Влияет на общий подход к ведению базы операционного риска в Банке**
		ВСР.3.7. Обеспечение целостности и доступности данных, содержащихся в базе событий, а также сохранности данных о потерях и возмещениях	
		ВСР.3.8. Протоколирование и контроль внесения изменений в базу событий	

ГОСТ 57580.4

	Процесс	Требования	Следствие
1	**Идентификация критичной архитектуры**	**ИКА.1.5.** Организация и выполнение деятельности по учету элементов критичной архитектуры: объектов информатизации *(прикладного и инфраструктурного уровней)* финансовой организации, задействованных при выполнении каждого из бизнес- и технологического процессов, в том числе их конфигураций	
2	**Управление изменениями**	**УИ.18.1.** Проведение регулярного контроля соответствия текущих конфигураций объектов информатизации стандартам конфигурирования, включая контроль со стороны службы ИБ, в целях контроля и выявления несанкционированного изменения текущих конфигураций объектов информатизации, а также их соответствия стандартам конфигурирования	
3	**Выявление, регистрация, реагирование на инциденты,** связанные с реализацией информационных угроз, и восстановление после их реализации	**ВРВ.14.1.** Включение в состав правил и процедур *(playbooks)* реагирование на инциденты, в том числе процедур приоритизации, эскалации и принятия *(или делегирования прав по принятию)* решений в рамках реагирования на инциденты, в том числе на основе определенного уровня критичности инцидента	**Меры требуют технической реализации**
		ВРВ.20. Уничтожение всех вредоносных элементов *(артефактов)* с объектов информатизации, в отношении которых реализовался инцидент, после сбора и фиксации технических данных *(свидетельств)*	
		ВРВ.26.7. Включение в состав правил и процедур (playbooks) восстановления функционирования бизнес- и технических процессов и объектов информатизации после реализации инцидентов: процедур сбора и фиксации технических данных *(свидетельств)* в рамках восстановления после реализации инцидентов для анализа причин и последствий реализации инцидентов	

ГОСТ 57580.4

	Процесс	Требования	Следствие
4	**Выявление, регистрация, реагирование на инциденты,** связанные с реализацией информационных угроз, и восстановление после их реализации	**ВРВ.32.** Организация и выполнение деятельности по сбору и фиксации технических данных *(свидетельств)* в рамках восстановления функционирования бизнес- и технических процессов и объектов информатизации после реализации инцидентов, в том числе во взаимодействии с причастными сторонами, способом, обеспечивающим юридическую значимость собранных технических данных *(свидетельств)*	
5	**Взаимодействие с поставщиками услуг**	**ВПУ.3.6.** Определение процедур по обеспечению безопасности цепи поставок *(для целей обеспечения операционной надежности)* в отношении поставщиков услуг, входящих в критичную архитектуру, включая предварительную оценку *(испытание, тестирование)* объектов информатизации перед их использованием в качестве элементов критичной архитектуры *(на этапах подбора или принятия в эксплуатацию, а также при их модернизации)*	**Меры требуют технической реализации**
		ВПУ.12.4. Своевременное, планируемое и контролируемое техническое обслуживание объектов информатизации прикладного и инфраструктурного уровней, входящих в критичную архитектуру, в том числе тестирование *(проверка)* работоспособности объектов информатизации после проведения технического обслуживания для выявления риска нарушения операционной надежности	
		ВПУ.13.5, 13.6, 13.8. Контроль удаленного технического обслуживания и диагностики, осуществляемых при подключении извне вычислительных сетей финансовой организации, в том числе предусматривающих: • Установление в договорах *(контрактах)* требований к осуществлению удаленного технического обслуживания и диагностики только по средством объектов информатизации , в отношении которых реализован тот же уровень защиты *(в том числе защиты информации),* который применяется для обслуживаемых объектов информатизации • Использование защищенного выделенного *(виртуального)* канала сетевого взаимодействия при удаленном техническом обслуживании • Контроль и подтверждение завершения сессии и прерывания сетевого подключения субъектов доступа после окончания удаленного технического обслуживания и диагностики	

Выводы

- ОН неразрывна с управлением риском
- ГОСТ, который мы внедряли последние 4 года, – это маленькая часть всех новых требований
- Новые ГОСТы ещё не обязательны, но пора разрабатывать план их реализации
- ГОСТы содержат больше организационных мер, чем технических. Их вес для оценки ещё не известен, но по традиции технические меры весят больше
- Рекомендую включить Требования ГОСТов в план годовой оценки ОР на 2023
- ОН реализуется в связке ИБ + ИТ + ОР, нужно выстроить эффективные процессы между функциями
- Базу ОР в exel вести уже нельзя, технических решений на рынке мало *(проблема для отрасли)*
- На поставщиков так же распространяются требования ОН *(требуется аудит ГОСТ)*
- Не всегда можно найти альтернативного поставщика для критического аутсорсинга *(проблема для отрасли)*

AKTIV.
CONSULTING

БЛАГОДАРЮ
ЗА ВНИМАНИЕ!

Фаина Митрофанова

Независимый эксперт
по информационной безопасности

+7 (987) 430-91-20

AKTIV.CONSULTING

БЛАГОДАРИМ
ЗА ВНИМАНИЕ

#бизнес-завтрак
24 мая