Применение результатов реализации 187-ФЗ для совершенствования кибербезопасности субъекта КИИ

Зуев Владимир, АО «Россельхозбанк»

Июль 2021 год

'21 МЕНЯЕМСЯ ВМЕСТЕ
RSHB.RU

Начальные шаги по реализации Федерального закона № 187-ФЗ

Основные нормативные документы для начала процесса категорирования

- Федеральный закон от 26.07.2017 № 187-ФЗ
- Постановление Правительства РФ от 08.02.2018 № 127

Нормы пункта 5 Постановления Правительства РФ № 127, дающие службе безопасности возможность детально изучить процессы организации

- а) **определение процессов**, указанных в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;
- б) **выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов** в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - **критические процессы**);
- в) определение объектов критической информационной инфраструктуры, которые **обрабатывают информацию, необходимую для обеспечения критических процессов**, и (или) осуществляют **управление, контроль или мониторинг критических процессов**;

'21 МЕНЯЕМСЯ ВМЕСТЕ

Первая реакция бизнеса при знакомстве с 187-ФЗ

Закон о безопасности - всё должна делать безопасность

↓

Должна ли безопасность самостоятельно провести все мероприятия, связанные с категорированием?

↓

НЕ ДОЛЖНА

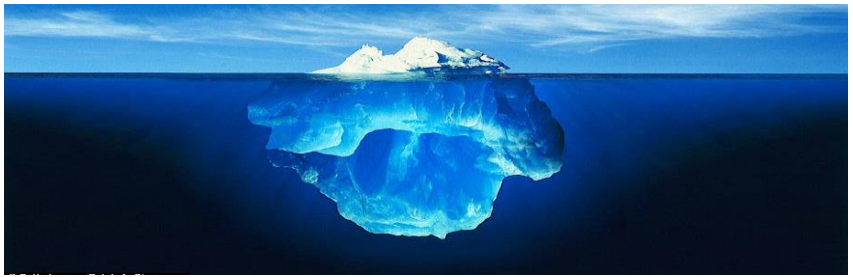
'21 МЕНЯЕМСЯ ВМЕСТЕ

Определение процессов организации и выявление среди них критических

«Формальный» подход

- Учредительные документы;
- Устав;
- Иные положения организации;
- ОКВЭД;
- ЕГРЮЛ/ЕГРИП.

В итоге имеем несколько десятков объемных верхнеуровневых процессов, включающих в себя множество ИС, АСУ, ИТС



Детальный подход

- Изучение классификаторов типовых процессов, характерных для сферы, в которой функционирует субъект КИИ;
- Анализ организационной структуры субъекта КИИ и положений о подразделениях;
- Запрос в подразделение субъекта КИИ, занимающееся планированием стратегической деятельности субъекта КИИ, на предмет существования перечня процессов организации.

В итоге имеем несколько сотен детализированных процессов, включающих в себя конкретные ИС, АСУ, ИТС

'21 МЕНЯЕМСЯ ВМЕСТЕ

Преимущества детального подхода

- Четкое отнесение ИС, АСУ, ИТС к этапам критического процесса\критическим процессам;
- Приобретение ценных данных о бизнес составляющей организации и о том, что имеет реальную важность и ценность для бизнеса (в защиту чего бизнес готов и желает инвестировать, а не вынужден и сопротивляется потому что так сказали);
- Улучшение понимания того, что именно мы защищаем (процессы бизнеса и обеспечивающие их системы уже не черная коробка);
- Выстраивание диалога с бизнесом, необходимого как на дальнейших этапах реализации категорирования, так и при построении гибкой системы защиты (возможность для безопасности выйти из роли «надсмотрщиков»);
- Возможность продвигать необходимость структуризации процессов организации в рамках реализации требований законодательства Российской Федерации (взаимовыгодно как владельцам процессов, у которых всегда есть такая потребность, так и безопасности, которая окажет реальное содействие развитию организации в целом);

'21 МЕНЯЕМСЯ ВМЕСТЕ

Важность исследования процессов

Какие результаты исследования процессов можно использовать?

- Схема процесса – ценное знание, позволяющее отслеживать его состояние не только в рамках бизнес метрик, но и при имплементации мер защиты;
- Владелец процесса – источник информации об его узких местах, которые могут не быть видны безопасности, смотрящей на процесс «извне»;
- Метрики процесса, полученные в рамках его анализа (входные, выходные данные (объем, количество, тип, время), скорость его исполнения, и т.п.) – подспорье во внедрение более точных мер контроля (как ручных, так и автоматизированных).

Что является необходимостью для реализации такого подхода?

- Наличие процессов периодической инвентаризации информационной инфраструктуры со стороны ИТ и ИБ;
- Наличие схем процессов организации (особенно тех, что попали в понимании Федерального закона № 187-ФЗ в категорию критических);
- Понимание обоюдной потребности к диалогу между безопасностью и владельцами процессов;
- Смена роли служб безопасности от «продавцов страха» к тем, кто реально обеспечивает потребности бизнеса в части безопасности.

'21 МЕНЯЕМСЯ ВМЕСТЕ

Что это может дать службе безопасности?

- Гибкий и детальный анализ на данном этапе может стать крепким фундаментом к эволюционному развитию служб кибербезопасности и усложнению их структуры, а также возможности организации своих центров мониторинга ИБ;

- Возможность взглянуть на свою деятельность под другим углом, оценить распределение собственных ресурсов/объем решаемых задач (основываясь на конкретных метриках процессов, в которые интегрируются меры защиты) и «сверить» его с реальными потребностями бизнеса, защита которого наверняка является приоритетной задачей для любой службы безопасности;

- Изменение статуса службы обеспечения кибербезопасности в глазах других подразделений организации;

'21 МЕНЯЕМСЯ ВМЕСТЕ

Выводы

- Начальные шаги реализации 127-ПП по определению процессов могут в дальнейшем дать субъекту больше информации для построения живой и гибкой системы защиты;
- Инвентаризация активов и наличие актуальных схем информационной инфраструктуры со стороны ИТ и ИБ крайне важно;
- Актуальные схемы процессов, в которых функционирует объект защиты, имеют весомую роль в построении системы защиты;
- Диалог служб безопасности с бизнесом\владельцами процессов важен для более глубокого понимания ландшафта защиты и выявления его узких мест;
- Разделение процессов на этапы – больше гибких и актуальных мер защиты;
- Реализация гибких мер защиты на разных этапах процесса формирует потребность в выделении обособленных специалистов\подразделений для обеспечения мониторинга функционирования мер защиты;
- Фундаментальная подготовка, анализ и планирование является основой эволюции служб безопасности и возможности построения центров мониторинга.

'21 МЕНЯЕМСЯ ВМЕСТЕ

Спасибо за внимание!

E-mail: zuevvm@rshb.ru
Tg: @Kpzrr

'21 МЕНЯЕМСЯ ВМЕСТЕ