Информационная инфраструктура предприятия: требования законодательства и подходы к документированию

Вячеслав Аксёнов

«Приорбанк» ОАО

Объекты информационной инфраструктуры

критически важные объекты информатизации, информационные сети, **информационные системы**, информационные ресурсы и иные совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации, принадлежащие государственным органам и иным организациям на праве собственности, хозяйственного ведения, оперативного управления или на ином законном основании, за исключением объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты

Перечень терминов и их определений (приложение 2), утвержденный Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 "О кибербезопасности"

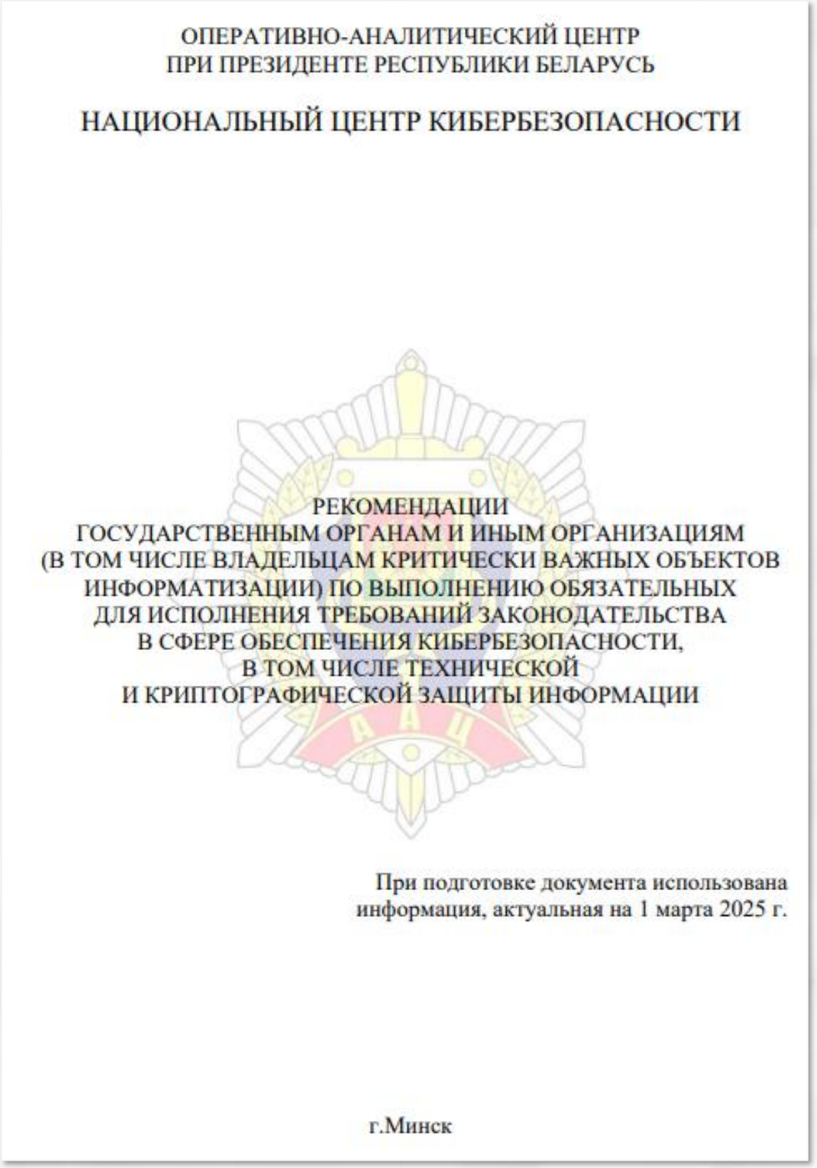
https://pravo.by/document/?guid=12551&p0=P32300040

Требования по защите

Кибербезопасность объектов информационной инфраструктуры (ОИИ)

Защита информации распространение и(или) предоставление которой ограничено (СЗИ)

Информационная безопасность критически важных объектов информатизации (КВОИ)



ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР
ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ

НАЦИОНАЛЬНЫЙ ЦЕНТР КИБЕРБЕЗОПАСНОСТИ

РЕКОМЕНДАЦИИ
ГОСУДАРСТВЕННЫМ ОРГАНАМ И ИНЫМ ОРГАНИЗАЦИЯМ
(В ТОМ ЧИСЛЕ ВЛАДЕЛЬЦАМ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ) ПО ВЫПОЛНЕНИЮ ОБЯЗАТЕЛЬНЫХ ДЛЯ ИСПОЛНЕНИЯ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ, В ТОМ ЧИСЛЕ ТЕХНИЧЕСКОЙ И КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

При подготовке документа использована информация, актуальная на 1 марта 2025 г.

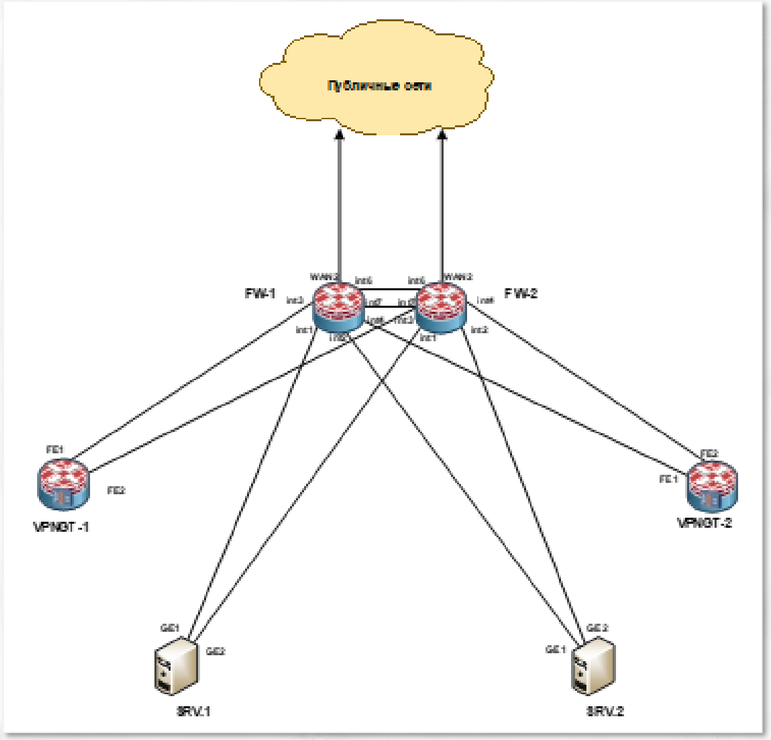
г.Минск

https://www.oac.gov.by/public/content/files/files/recom.pdf

Требования к документированию ИС

Структурная схема ИС отражает особенности функционирования ИС на **физическом и канальном уровнях** и должна содержать**:**

- наименование ИС;
- места размещения физических устройств, относящихся к активам ИС, средств ЗИ с указанием названия устройства согласно его системному имени (серийный номер – для неуправляемого устройства), названий физических интерфейсов устройства;
- физические линии связи с указанием их типа (витая пара, волоконно-оптический кабель и др.), идентификаторы виртуальных локальных вычислительных сетей (VLAN ID);
- физические границы ИС.



К структурной схеме ИС должны прилагаться:

- сведения о назначении линий связи (передача данных или управление активами ИС, средствами ЗИ);
- перечень виртуальных локальных вычислительных сетей (VLAN) с указанием их идентификаторов (VLAN ID), названий виртуальных локальных вычислительных сетей (VLAN Name), IP-адресации, используемой в виртуальных локальных вычислительных сетях (VLAN);
- перечень телекоммуникационного оборудования с указанием производителя оборудования, его модели, системного имени (серийного номера для неуправляемого устройства), IP-адреса управления устройством, места размещения (помещение, номер стойки, место в стойке и др.).

Объект	Сетевой порт	Линия связи	Сетевой порт	Объект

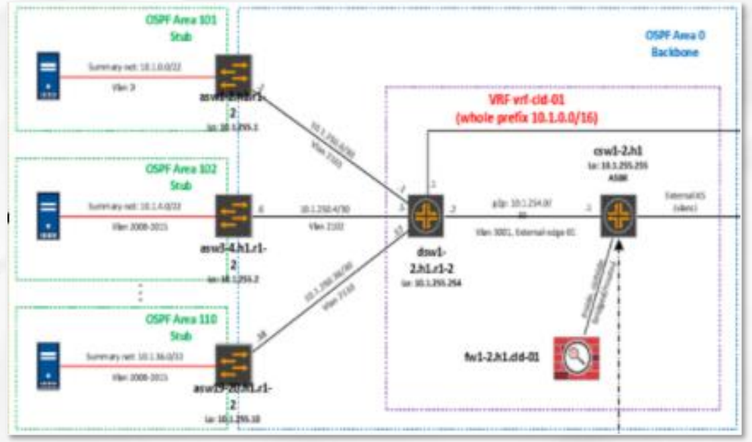
Наименование	Системное имя	IP-адрес	Место размещения

VLAN ID	VLAN Name	IP-адресация	Примечание

Требования к документированию ИС

Логическая схема ИС отражает особенности функционирования ИС на **сетевом и последующих уровнях** и должна содержать:

- ❑ наименование ИС;
- ❑ направления информационных потоков (внутренних и внешних). Для ИС классов «3-ин», «3-спец», «3-бг», «3-дсп» и «3-юл» допускается взаимодействие с любыми ИС;
- ❑ логические границы ИС.



Средство защиты	IP-адрес администрирования

IP-адрес	TCP/UDP порт	Сервис

Объект	Системное имя	IP-адрес

К логической схеме ИС должны прилагаться сведения:

- ❑ об информационных ресурсах, входящих в состав ИС, с указанием IP-адресов и названий физических серверов, виртуальных машин, контейнеров, обеспечивающих их функционирование;
- ❑ о средствах ЗИ с указанием IP-адресов их администрирования;
- ❑ об открытых портах транспортного уровня с указанием соответствующих им IP-адресов технологий и (или) протоколов.

Требования к документированию ОИИ

структурная схема объекта информационной инфраструктуры (расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программных, программно-аппаратных средств, в том числе средств защиты информации, автоматизированных рабочих мест администратора (оператора);

логическая схема объекта информационной инфраструктуры (информационные системы, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств);

направление информационных потоков с указанием узлов сети, имеющих внешнее информационное взаимодействие;

список используемых доменных имен и IP-адресов, посредством которых осуществляется внешнее информационное взаимодействие

Требования к документированию КВОИ

Форма

_____
(наименование владельца критически важного объекта информатизации)

Для служебного пользования
Экз. №

УТВЕРЖДАЮ

_____
(наименование должности

_____
руководителя организации)

_____
(подпись, инициалы, фамилия)
___.__.20___

ФОРМУЛЯР КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

_____
(наименование критически важного объекта информатизации)

1. Общие сведения о критически важном объекте информатизации:
наименование критически важного объекта информатизации;
место нахождения критически важного объекта информатизации;
критерий (критерии) отнесения объекта информатизации к критически важным объектам информатизации;
показатель (показатели) уровня вероятного ущерба национальным интересам Республики Беларусь;
подразделение (должностное лицо), ответственное за проведение работ по технической и криптографической защите информации, обрабатываемой на критически важном объекте информатизации;
сведения о вводе объекта информатизации в эксплуатацию.
2. Сведения об оборудовании и программном обеспечении, входящем в состав активов критически важного объекта информатизации:

№ п/п	Тип (вид)	Наименование, заводской (инвентарный) номер	Текущая версия программного обеспечения (сертификат соответствия)	Дата ввода в эксплуатацию	Ответственные лица
1	Программно-аппаратные средства и физические устройства				
2	Программное обеспечение (прикладное и системное)				
3	Средства защиты информации				
4	Информационные системы и информационные сети				
5	Средства обработки информации (потоков информации), средства коммуникации				
6	Средства администрирования и				

	конфигурирования				

3. Схема расположения критически важного объекта информатизации (с указанием конкретного здания, сооружения, помещения, этажа и тому подобного).
4. Структурная схема критически важного объекта информатизации (с указанием расположения физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации, средств защиты информации, автоматизированного рабочего места администратора (оператора).
5. Логическая схема критически важного объекта информатизации (с указанием информационных систем, направления потоков данных, а также спецификации используемых технологий и протоколов, списков VLAN, IP-адресов устройств).
6. Схема администрирования критически важного объекта информатизации.

Приложение 1 к Положению о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации
Приказ Оперативно-аналитического центра при Президенте Республики Беларусь 20.02.2020 № 66

ОИИ + ИС + КВОИ

Сведения	ИС	ОИИ	КВОИ
структурная схема	+	+	+
логическая схема	+	+	+
направление информационных потоков с указанием узлов сети, имеющих внешнее информационное взаимодействие		+	
список используемых доменных имен и IP-адресов, посредством которых осуществляется внешнее информационное взаимодействие		+	
схема расположения			+
схема администрирования			+
детальные сведения об оборудовании и ПО			+

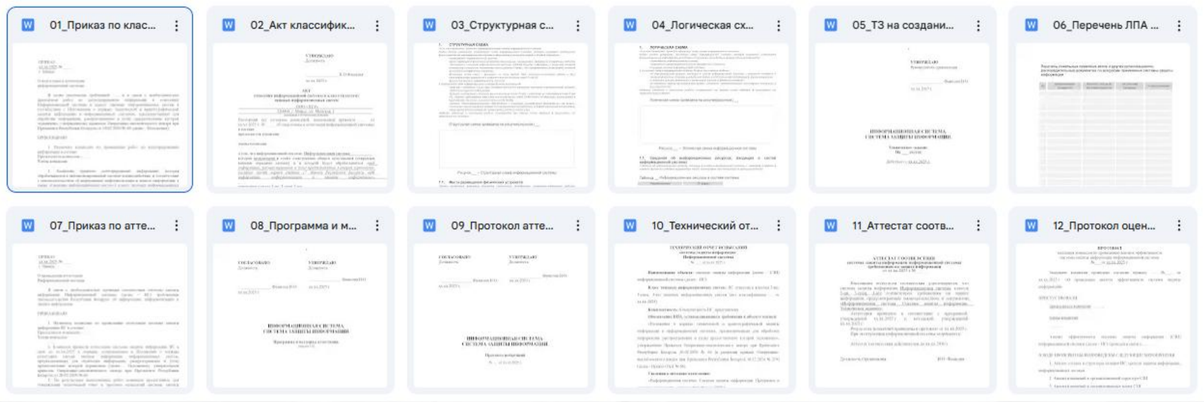
Подходы к документированию

Отдельные документы

Составной документа (паспорт/формуляр/общее описание)

Формализация процесса документирования и требований к сведениям (ЛПА)

Дополнительные материалы



п.п. Приказа	Этап проекта	Статус
	Классификация информационной системы	
7	Категорирование информации, которая будет обрабатываться в информационной системе, в соответствии с законодательством об информации, информатизации и защите информации, а также отнесение информационной системы к классу типовых информационных систем согласно приложению 1	Выполнено
7	Оформление акта классификации по форме согласно приложению 2	Выполнено
	Проектирование системы защиты информации	
8	Анализ структуры информационной системы и информационных потоков (внутренних и внешних) в целях определения состава (количества) и мест размещения элементов информационной системы (аппаратных и программных), ее физических и логических границ	не выполнено
9	Издание политики информационной безопасности	не выполнено
10	Определение требований к системе защиты информации в техническом задании на создание системы защиты информации	не выполнено
8	Выбор средств технической и криптографической защиты информации	Не выполнено
11	Разработка (корректировка) общей схемы системы защиты информации	Не выполнено
	Создание системы защиты информации	
16	Внедрение средств технической и криптографической защиты информации, проверка их работоспособности и совместимости с другими объектами информационной системы	Не выполнено
17, 18	Разработка (корректировка) документации на систему защиты информации по перечню, определенному в техническом задании	Не выполнено
19	Проведение предварительных испытаний	Не выполнено

Статус	Значение	Реализация проекта	Реализация требований ТЗ на СЗИ
?Неизвестно	Еще не проверено	50%	90%
Не выполнено	Требование не выполнено	40%	6%
Выполнено	Требование выполнено, документировано, где необходимо используются организационные или технические меры защиты информации	10%	2%
Не применимо	Требование является рекомендуемым и принято решение о его исключении, или требование исключено в связи с отсутствием информационной систем соответствующего объекта (технологии) либо при условии согласования с СЗИ закрепления в таком техническом задании обоснованных компенсирующих мер	0%	2%
		Всего: 100%	100%

№ п.п.	Требование	Статус
1	**Аудит безопасности**	
1.1	Определение состава информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности, информация о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации и другие)	Неизвестно
1.2	Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	Не выполнено
1.3	Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	Не выполнено
1.4	Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы	Выполнено
1.5	Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года	Не выполнено

Спасибо за внимание!