Приказ ОАЦ №259.
Изменения в требованиях законодательства Республики Беларусь в области защиты информации

Вячеслав Аксёнов
Enterprise Security Architect

2. Проектирование, создание и (или) аттестация систем защиты информации информационных систем, осуществляемые на основании договоров, заключенных до вступления в силу настоящего приказа, но не исполненных на дату вступления его в силу:

осуществляются в соответствии с законодательством, действовавшим на дату заключения указанных договоров;

по решению собственников (владельцев) информационных систем могут осуществляться в соответствии с настоящим приказом, если иное не предусмотрено законодательными актами.

3. Настоящий приказ вступает в силу в следующем порядке:

подпункт 1.2 пункта 1 и пункт 2 – с 1 марта 2025 г.;

иные положения настоящего приказа – после его официального опубликования.

Изменены требования к содержанию политики ИБ, и составу и содержанию ЛПА и других ОРД по вопросам применения СЗИ.

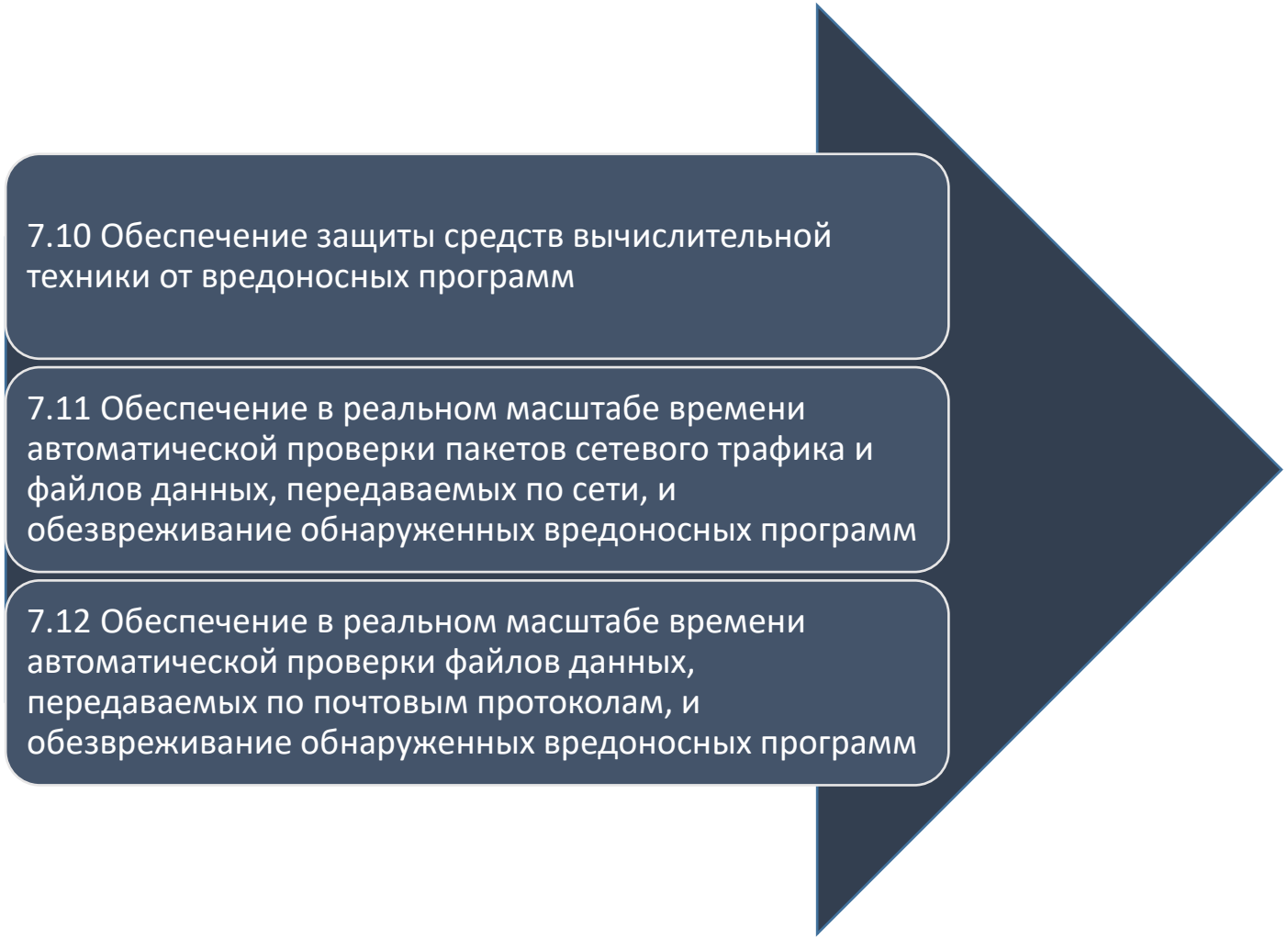
Требования сформулированы с учетом лучших международных практик по построению систем менеджмента ИБ и теперь **позволяют организации самостоятельно определять содержание и состав с учетом своей специфики** (например, размера организации и вида ее деятельности, сложности процессов и их взаимодействий и компетентности персонала).

Явно прописано **требование по утверждению** Политики ИБ, **Структурной и Логической схемы**, ТЗ на создание СЗИ, ЛПА по вопросам применения СЗИ, **собственником (владельцем) ИС**.

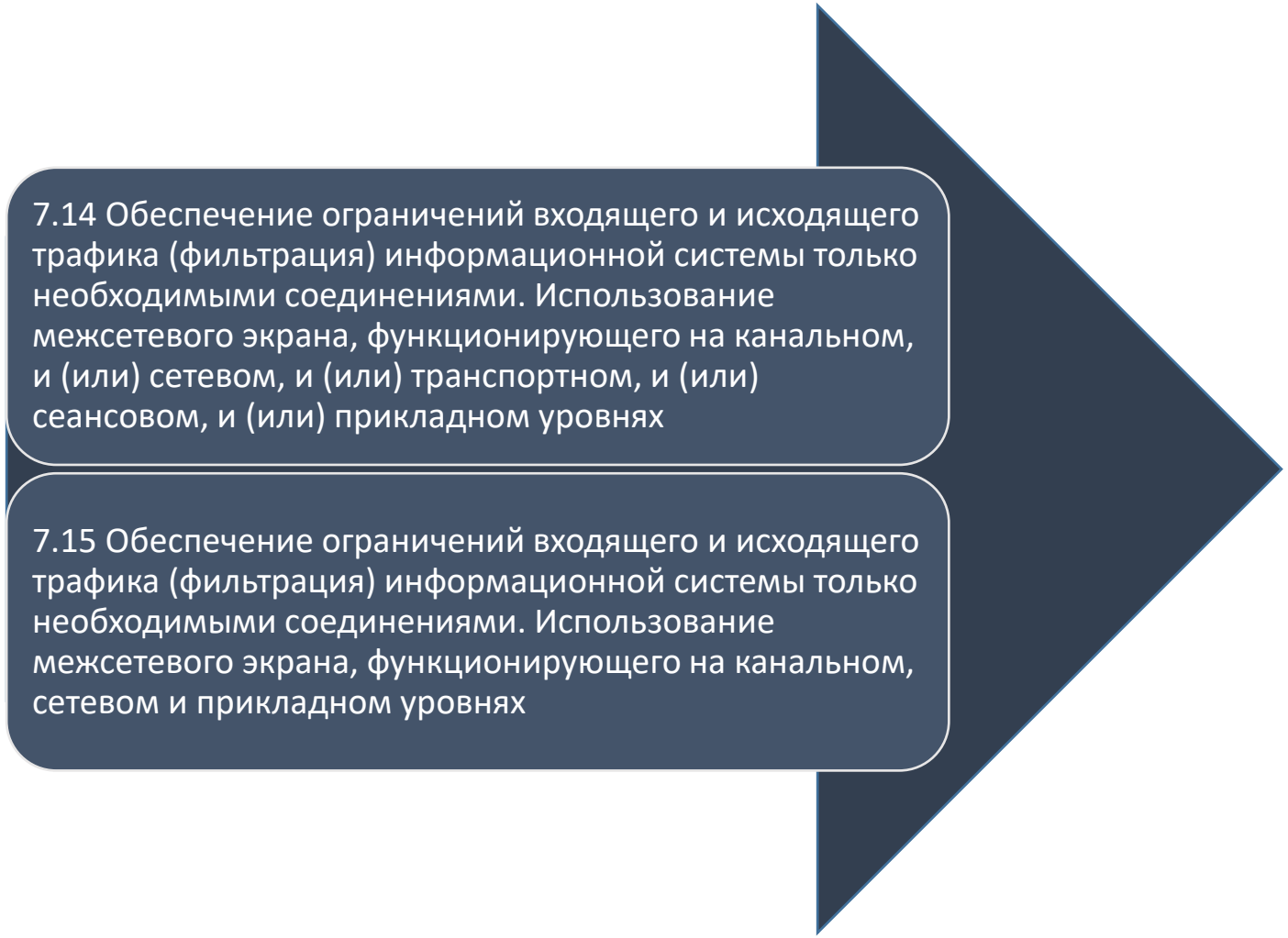
Установлен запрет на определение порядка применения СЗИ, в ЛПА организации по иным вопросам ее деятельности.

Добавлена необходимость проведения на регулярной основе, но не реже одного раза в год со дня аттестации СЗИ, **анализа эффективности применения СЗИ** (**результаты** Анализа **должны быть отражены в документе** произвольной формы, который подлежит утверждению руководителем организации – собственника (владельца) ИС).

В Перечне требований к СЗИ, подлежащих включению в ТЗ, **произошли значительные изменения** в части добавления/исключения требований, уточнения/изменения формулировок требований, изменения области применения требований.



7.10
обеспечение защиты от воздействия вредоносных программ



7.12
обеспечение межсетевого экранирования при информационном взаимодействии (внутреннем и внешнем) по протоколам сетевого и транспортного уровней

7.21 Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы

7.17 ежегодное проведение оценки эффективности защищенности информационной системы (тестирование на проникновение)

Добавлены новые требования:	5.7 издание сертификатов открытых ключей проверки электронной цифровой подписи (удостоверяющий центр, регистрационный центр (при его наличии), средства электронной цифровой подписи)
	7.18 обеспечение обнаружения и реагирования на угрозы безопасности конечных узлов (уровня узла) в информационной системе
	7.19 обеспечение централизованного сбора и хранения сведений о DNS-запросах активов информационной системы, средств защиты информации в течение установленного срока хранения, но не менее одного месяца

7.19
Определение перечня внешних подключений к информационной системе и порядка такого подключения

уточнения/изменения формулировок требований,
изменения области применения требований.

Было	Стало
Информация о событиях информационной безопасности	Сведения о событиях информационной безопасности
Сетевое оборудование	Телекоммуникационное оборудование
Объекты информационной системы	Активы информационной системы
Резервирование	Резервное копирование

Легенда:
Требование осталось неизменным
Изменена формулировка требования
Требование исключено
Требование заменено на более строгое
Требование заменено более общим требованием
Новое требование

Требование		**Применимость**																			
		Было										**Стало**									
Было	**Стало**	**4-ин**	**4-спе**	**4-бг**	**4-юл**	**4-дсп**	**3-ин**	**3-спе**	**3-бг**	**3-юл**	**3-дсп**	**4-ин**	**4-сп**	**4-бг**	**4-юл**	**4-дс**	**3-ин**	**3-сп**	**3-бг**	**3-юл**	**3-дсп**
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 другое)	1.1 определение состава **сведений о событиях** информационной безопасности, подлежащих регистрации	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.2 Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	1.2 обеспечение сбора и хранения **сведений о событиях** информационной безопасности в течение установленного срока хранения, но не менее одного года	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1.3 Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	1.3 обеспечение централизованного сбора и хранения **сведений о событиях** информационной безопасности в течение установленного срока хранения, но не менее одного года			x			x	x	x		x			x			x	x	x	x	x

Добавлено **требование проводить** оценку эффективности защищенности ИС **(тестирование на проникновение) в ходе аттестации СЗИ** для систем класса «3-бг» и «3-дсп».

Добавлены **требования к содержанию технического отчета и протокола испытаний**.

Изменилась частота предоставления сведений:

- об ИС, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам;
- о подразделениях защиты информации или иных подразделениях (должностных лицах), ответственных за обеспечение защиты информации.

Теперь данные сведения дополнительно **предоставляются не позднее десяти календарных дней с момента изменения ранее представленных сведений**.

Детальные сведения об изменениях

Изменения в Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

В Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, были внесены следующие изменения:

1. **Добавлены определения следующих терминов**: активы информационной системы, защищенный канал передачи данных, компрометация криптографического ключа.

2. Из Приложения 1 ,которое содержит Классы типовых информационных систем, **исключены классы «6-част», «6-гос», «5-част», «5-гос»**.

3. В приложении 2 **внесены изменения в форму Акта отнесения** информационной системы к классу (классам) типовых ИС.

4. В этап проектирования системы защиты информации внесены следующие изменения:

4.1 Проектирование СЗИ начинается с **разработки (корректировки) политики ИБ** (ранее первым этапом был **анализ структуры ИС** 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.

Добавлен этап «разработка проектов локальных правовых актов и других организационно распорядительных документов по вопросам применения системы защиты информации», а также требование по утверждению Политики ИБ, Структурной и Логической схемы, ТЗ на создание СЗИ, ЛПА по вопросам применения СЗИ, собственником (владельцем) информационной системы.

Исключены такие этапы как:

- выбор средств технической и криптографической защиты информации;
- разработка (корректировка) общей схемы системы защиты информации.

4.2 В таблице 1 представлены **изменения требований к содержанию политики ИБ**. Теперь эти **требования позволяют организации самостоятельно определять содержание политики с учетом своей специфики**.

Таблица 1 – Сравнение требований к содержанию Политики ИБ

Было	Стало
цели и принципы защиты информации	цели и принципы защиты информации
перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем, перечень средств вычислительной техники, а также сведения о подразделении защиты информации или ином подразделении (должностном лице), ответственном за обеспечение защиты информации (если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами);	-

Было	Стало
обязанности пользователей информационной системы	Теперь обязанности должны быть определены в ЛПА по применению СЗИ
порядок взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия), в том числе при осуществлении информационных отношений на правах операторов, посредников, пользователей информационных систем и обладателей информации	-
-	обязательства собственника (владельца) информационной системы соответствовать требованиям по защите информации, постоянно совершенствовать систему защиты информации.
-	**по решению собственника (владельца) информационной системы может содержать иную информацию,** отражающую общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, обрабатываемой в информационной системе
-	должна быть доведена до сведения работников собственника (владельца) информационной системы в части, их касающейся, быть доступной всем заинтересованным субъектам информационных отношений для ознакомления

4.3. Теперь установлено, что сразу после разработки (корректировки) политики ИБ на основе анализа структуры ИС и информационных потоков (внутренних и внешних), состава, количества и мест размещения активов информационной системы, ее физических и логических границ разрабатываются Структурная и логическая схемы информационной системы. Интересно, что **если сравнить с требованиями к содержанию структурной и логической схем, которые содержатся в Положении о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, а также в Приказе ОАЦ №130, то, на мой взгляд требования к содержанию таких схем в редакции Приказа №259 самые строгие и детальные**.

4.4. В таблице 2 представлены изменения в **требованиях к содержанию Технического задания** на создание СЗИ.

Таблица 2 – Сравнение требований к содержанию ТЗ на создание СЗИ

Было	Стало
наименование информационной системы с указанием присвоенного ей класса типовых информационных систем	наименование информационной системы с указанием присвоенного (присвоенных) ей класса (классов) типовых информационных систем
требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3	требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3
сведения об организации взаимодействия с иными информационными системами (в случае предполагаемого взаимодействия) с учетом требований согласно приложению 4	-
порядок обезличивания персональных данных (в случае их обработки в информационной системе) с применением методов согласно приложению 5	порядок обезличивания персональных данных, если предполагается обезличивание персональных данных. Допустимые методы обезличивания определены согласно приложению 4
требования из числа реализованных в аттестованной в установленном порядке системе защиты информации информационной системы другого собственника (владельца) – если функционирование информационной системы, для которой осуществляется проектирование системы защиты информации, предполагается на базе информационной системы другого собственника (владельца) в соответствии с пунктом настоящего Положения	требования из числа реализованных в аттестованной в установленном порядке системе защиты информации информационной системы другого собственника (владельца), если функционирование информационной системы, для которой осуществляется проектирование системы защиты информации, предполагается на базе информационной системы другого собственника (владельца) в соответствии с пунктом 15 настоящего Положения
требования к средствам криптографической защиты информации, включая требования к криптографическим алгоритмам в зависимости от задач безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита), криптографическим протоколам, управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям безопасности и форматам данных. Профили требований, предъявляемых к средствам криптографической защиты информации, определяются Оперативно-	требования к средствам криптографической защиты информации на основе перечня государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденным постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375

СПАСИБО ЗА ВНИМАНИЕ!