КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Опыт построения систем защиты информации в соответствии с требованиями законодательства: ошибки проблемы спорные моменты

Вячеслав Аксёнов
менеджер по ИБ «Приорбанк» ОАО

Зачем это все надо?

Закон Республики Беларусь
от 10 ноября 2008 г. № 455-З
«Об информации, информатизации и защите информации»

Статья 28. Основные требования по защите информации

- **Информация, распространение** и (или) предоставление **которой ограничено**, не отнесенная к государственным секретам, **должна обрабатываться** в информационных системах **с применением системы ЗИ, аттестованной в порядке, установленном ОАЦ**

Закон РБ от 07.05.2021 г. № 99-З
«О защите персональных данных»

Статья 17. Меры по обеспечению защиты персональных данных

3. **Обязательными мерами по обеспечению защиты персональных данных являются**:

- **осуществление** технической и криптографической **защиты персональных данных в порядке, установленном Оперативно-аналитическим центром** при Президенте Республики Беларусь, в соответствии с классификацией информационных ресурсов (систем), содержащих персональные данные.

Кодекс Республики Беларусь об административных правонарушениях

Статья 23.7 часть 4
Несоблюдение мер обеспечения защиты персональных данных физических лиц
– влечет наложение штрафа в размере от двух до десяти базовых величин, на индивидуального предпринимателя – от десяти до двадцати пяти базовых величин, а на юридическое лицо – **от двадцати до пятидесяти базовых величин**.

Закон РБ от 10.11.2008 г. № 455-З
«**Об информации, информатизации и защите информации**»

Закон РБ от 05.01.2013 г. № 16-З
«**О коммерческой тайне**»

Закон РБ от 07.05.2021 г. № 99-З
«О защите персональных данных»

Положение о технической и криптографической защите информации
Указ Президента РБ от 16.04.2013 № 196 (в редакции Указа Президента РБ от 09.12.2019 № 449)

О служебной информации ограниченного распространения и информации, составляющей коммерческую тайну
Постановление Совета Министров РБ от 12 августа 2014 г. № 783

Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)
Постановление Совета Министров РБ 15.05.2013 № 375 (в редакции постановления Совета Министров РБ 12.03.2020 № 145)

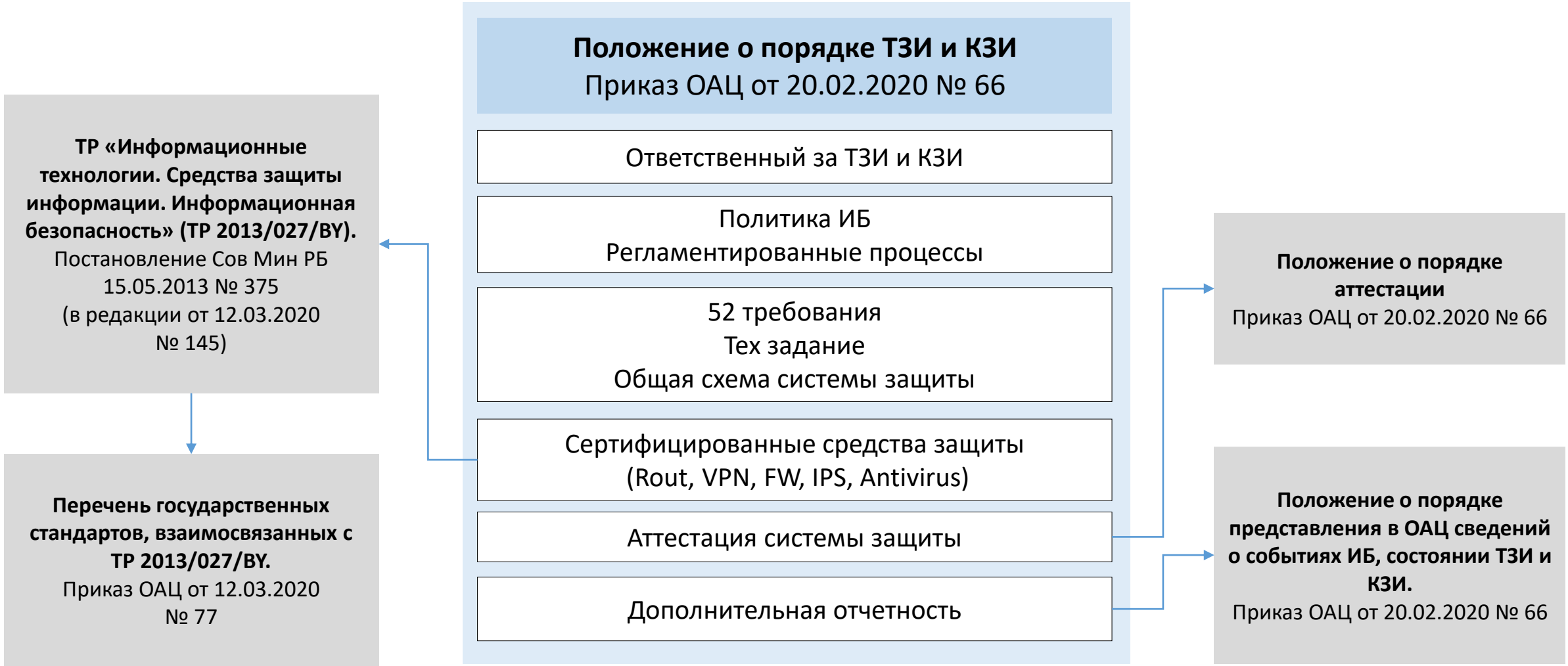
Перечень государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY)
Приказ ОАЦ от 12.03.2020 № 77

Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено
Приказ ОАЦ от 20.02.2020 № 66 (в редакции приказа от 12.11.2021 № 195)

Положение о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации
Приказ ОАЦ от 20.02.2020 № 66 (в редакции приказа от 12.11.2021 № 195)

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено
Приказ ОАЦ от 20.02.2020 № 66

Техническая и криптографическая защита



Приложение 1
Классы типовых информационных систем

Классификация ИС

Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено
Приказ ОАЦ от 20.02.2020 № 66 (в редакции приказа от 12.11.2021 № 195)

Категория информации (форма собственности ИС)		Наличие подключения к открытым каналам передачи данных	
		есть	**нет**
общедоступная информация (в т.ч. общедоступные персональные данные	государственная ИС	5-гос	6-гос
	негосударственная ИС	5-частн	6-частн
персональные данные, за исключением специальных персональных данных		3-ин	**4-ин**
специальные персональные данные, за исключением биометрических и генетических персональных данных		3-спец	**4-спец**
биометрические и генетические персональные данные		3-бг	**4-бг**
информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения)		3-юл	**4-юл**
служебная информация ограниченного распространения		3-дсп	**4-дсп**

Техническое задание

Техническое задание должно содержать:

наименование информационной системы с указанием присвоенного ей класса типовых информационных систем;

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

требования к средствам криптографической защиты информации;

перечень документации на систему защиты информации.

требования из числа реализованных в аттестованной в установленном порядке СЗИ ИС другого собственника (владельца)

Общая схема СЗИ

Общая схема СЗИ должна содержать:

- ❑ наименование ИС
- ❑ класс типовых ИС
- ❑ **места размещения** СВТ, сетевого оборудования, **системного и прикладного ПО**, средств технической и криптографической ЗИ
- ❑ физические границы ИС
- ❑ внешние и внутренние информационные потоки и протоколы обмена защищаемой информацией

Виды требований

встроенные средства системного и прикладного ПО

№ п.п.	Требование
1	**Аудит безопасности**
1.2	Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года
3	**Требования по обеспечению идентификации и аутентификации**
3.2	Обеспечение идентификации и аутентификации пользователей информационной системы
3.3	Обеспечение защиты обратной связи при вводе аутентификационной информации
3.4	Обеспечение полномочного управлени записями пользователей информацион
3.5	Обеспечение контроля за соблюдением информационной системы
3.7	Обеспечение блокировки доступа к объ времени бездействия (неактивности) по

Организационные меры (регламентация)

№ п.п.	Требование
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)
2	**Требования по обеспечению защиты данных**
2.1	Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контр
7	
7.1	Определение перечня разрешенного пр использования

Средства защиты информации

№ п.п.	Требование
5	**Обеспечение криптографической защиты информации**
5.1	Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного шифрования), если не осуществлено предварительное шифрование защищаемой информации
7	**Иные требования**
7.10	Обеспечение защиты средств вычислительной техники от вредоносных программ
7.14	Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях
7.18	Обеспечение обнаружения утечек информации из информационной системы. Использование системы обнаружения утечек информации из информационной системы

Использование средств ЗИ

ПЕРЕЧЕНЬ
требований к системе защиты информации, подлежащих включению в техническое задание

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом типовых информационных систем									
		4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	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)	+	+	+	+	+	+	+	+	+	+
1.2	Обеспечение 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 информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+/–	+/–	+	+/–	+/–	+	+	+	+/–	+

ПО должно быть сертифицировано в качестве средства защиты

Использование средств ЗИ

ТР «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).
Постановление Сов Мин РБ 15.05.2013 № 375
(в редакции от 12.03.2020
№ 145)

→

Перечень государственных стандартов, взаимосвязанных с ТР 2013/027/BY.
Приказ ОАЦ от 12.03.2020
№ 77

Перечень требований к СЗИ (приложение 3)

5	**Обеспечение криптографической защиты информации**
5.1	Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного шифрования), если не осуществлено предварительное шифрование защищаемой информации
5.2	Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)
5.3	Обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)
5.4	Обеспечение контроля целостности данных в информационной системе (средства контроля целостности)
5.5	Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены)
5.6	Обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в информационной системе (криптографический токен и (или) средства выработки электронной цифровой подписи)

7.10	Обеспечение защиты средств вычислительной техники от вредоносных программ
7.11	Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ
7.12	Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ
7.13	Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего)
7.14	Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях
7.15	Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях
7.16	Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений
7.17	Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений
7.18	Обеспечение обнаружения утечек информации из информационной системы. Использование системы обнаружения утечек информации из информационной системы
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

Криптографическая защита биометрических и генетических персональных данных

5.2 Обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)

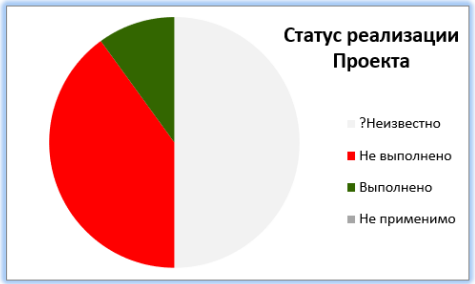
5.4 Обеспечение контроля целостности данных в информационной системе (средства контроля целостности)

Необходимость замены средств защиты информации, на которые истек срок действия сертификата ОАЦ (серийное производство)?

Дополнительные материалы

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 системе соответствующего объекта (технологии) либо при условии согласования с ОАЦ 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 другое)	?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



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	Реализация организационных мер по защите информации	Не выполнено

https://drive.google.com/drive/folders/1dICi0JD-X6TxaDKQGeSA6efvkOG2xXbx

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

СПАСИБО ЗА ВНИМАНИЕ!

Вячеслав Аксёнов
менеджер по ИБ «Приорбанк» ОАО