

# **ОСНОВЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ**

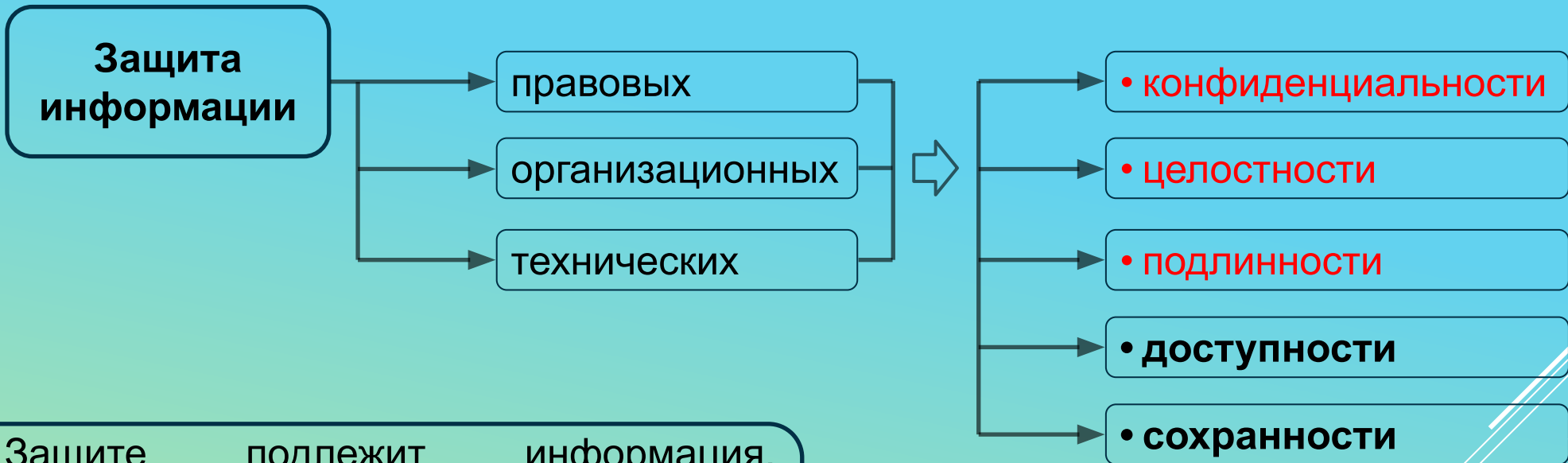
**СРЕДСТВА ЗАЩИТЫ  
ОТ НАРУШЕНИЙ**

**ВНУТРЕННИЕ И ВНЕШНИЕ  
НАРУШИТЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ**

**СРЕДСТВА ТЕХНИЧЕСКОЙ  
ЗАЩИТЫ ИНФОРМАЦИИ**

**СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ  
ЗАЩИТЫ ИНФОРМАЦИИ**

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



Защите подлежат информация, неправомерные действия в отношении которой могут причинить вред ее обладателю, пользователю или иному лицу.

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

Глава 3. Правовой режим информации  
Статья 15. Виды информации



Общедоступная информация



Информация, распространение и (или)  
предоставление которой ограничено

## Статья 16. Общедоступная информация

- о правах, свободах, законных интересах и обязанностях физических лиц, правах, законных интересах и обязанностях юридических лиц и о порядке реализации прав, свобод и законных интересов, исполнения обязанностей;
- о деятельности государственных органов, общественных объединений;
- о правовом статусе государственных органов, за исключением информации, доступ к которой ограничен законодательными актами;
- о социально-экономическом развитии Республики Беларусь и ее административно-территориальных единиц;
- о чрезвычайных ситуациях, экологической, санитарно-эпидемиологической обстановке, гидрометеорологической и иной информации, отражающей состояние общественной безопасности;
- о состоянии здравоохранения, демографии, образования, культуры, сельского хозяйства;
- о состоянии преступности, а также о фактах нарушения законности;
- о льготах и компенсациях, предоставляемых государством физическим и юридическим лицам;
- о размерах золотого запаса;
- об обобщенных показателях по внешней задолженности;
- о состоянии здоровья должностных лиц, занимающих должности, включенные в перечень высших государственных должностей Республики Беларусь;
- накапливаемой в открытых фондах библиотек и архивов, информационных системах государственных органов, физических и юридических лиц, созданных (предназначенных) для информационного обслуживания физических лиц.

## Статья 17. Информация, распространение и (или) предоставление которой ограничено

- сведения, **составляющие государственные секреты** (статья 14 Закона Республики Беларусь от 19.07.2010 № 170-3 «О государственных секретах»);
- **служебная информация ограниченного распространения** (статья 18<sup>1</sup> Закона № 455-3);
- информация **о частной жизни физического лица и персональные данные** (Закон Республики Беларусь от 7 мая 2021 г. № 99-3 «О защите персональных данных»);
- информация, составляющая **коммерческую, профессиональную, банковскую и иную охраняемую законом тайну**;
- информация, содержащаяся **в делах об административных правонарушениях, материалах и уголовных делах** органов уголовного преследования и суда до завершения производства по делу;
- иная информация, доступ к которой ограничен законодательными актами.

# Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»

**Персональные данные** – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано.

- Биометрические персональные данные
- Генетические персональные данные
- Общедоступные персональные данные
- Специальные персональные данные

**Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

## Глава 7. Защита информации. Статья 28. Основные требования по защите информации.



### Общедоступная информация.

Требования по защите общедоступной информации могут устанавливаться только в целях недопущения ее уничтожения, модификации (изменения), блокирования правомерного доступа к ней.

Защита сведений, составляющих

**государственные секреты** – Закон Республики Беларусь от 19.07.2010 № 170-З «О государственных секретах».



### Информация, распространение и (или) предоставление которой ограничено.

Информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, должна обрабатываться в **информационных системах** с применением **системы защиты информации, аттестованной** в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь.

Для создания **системы защиты информации** используются средства **технической** и **криптографической** защиты информации, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, порядок проведения которой определяется Оперативно-аналитическим центром при Президенте Республики Беларусь.

Не допускается эксплуатация государственных информационных систем без реализации мер по защите информации.



# **ВНУТРЕННИЕ И ВНЕШНИЕ НАРУШИТЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ**

Все источники угроз безопасности информации можно разделить на три основные группы:

- **антропогенные** (обусловленные действиями субъекта);
- **техногенные** (обусловленные техническими средствами);
- **стихийные** (обусловленные стихийными источниками).

В ходе оценки угроз безопасности информации рассмотрим **антропогенные** источники угроз безопасности информации, к которым относятся **лица (группа лиц)**, осуществляющие реализацию угроз безопасности информации путем **несанкционированного доступа** и (или) **воздействия (НСД/НСВ)** на информационные ресурсы и (или) компоненты систем и сетей, - нарушители.

## Основные виды нарушителей, подлежащие оценке:

- ✓ специальные службы иностранных государств;
- ✓ террористические, экстремистские группировки;
- ✓ преступные группы (криминальные структуры);
- ✓ отдельные физические лица (хакеры);
- ✓ конкурирующие организации;
- ✓ разработчики программных, программно-аппаратных средств;
- ✓ лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем;
- ✓ поставщики услуг связи, вычислительных услуг;
- ✓ лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ;
- ✓ лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.);
- ✓ авторизованные пользователи систем и сетей;
- ✓ системные администраторы и администраторы безопасности;
- ✓ бывшие (уволенные) работники (пользователи).

Для нарушителей должны быть определены их категории в зависимости от имеющихся прав и условий по доступу к системам и сетям, обусловленных архитектурой и условиями функционирования этих систем и сетей, а также от установленных возможностей нарушителей. При этом нарушители подразделяются на две категории:

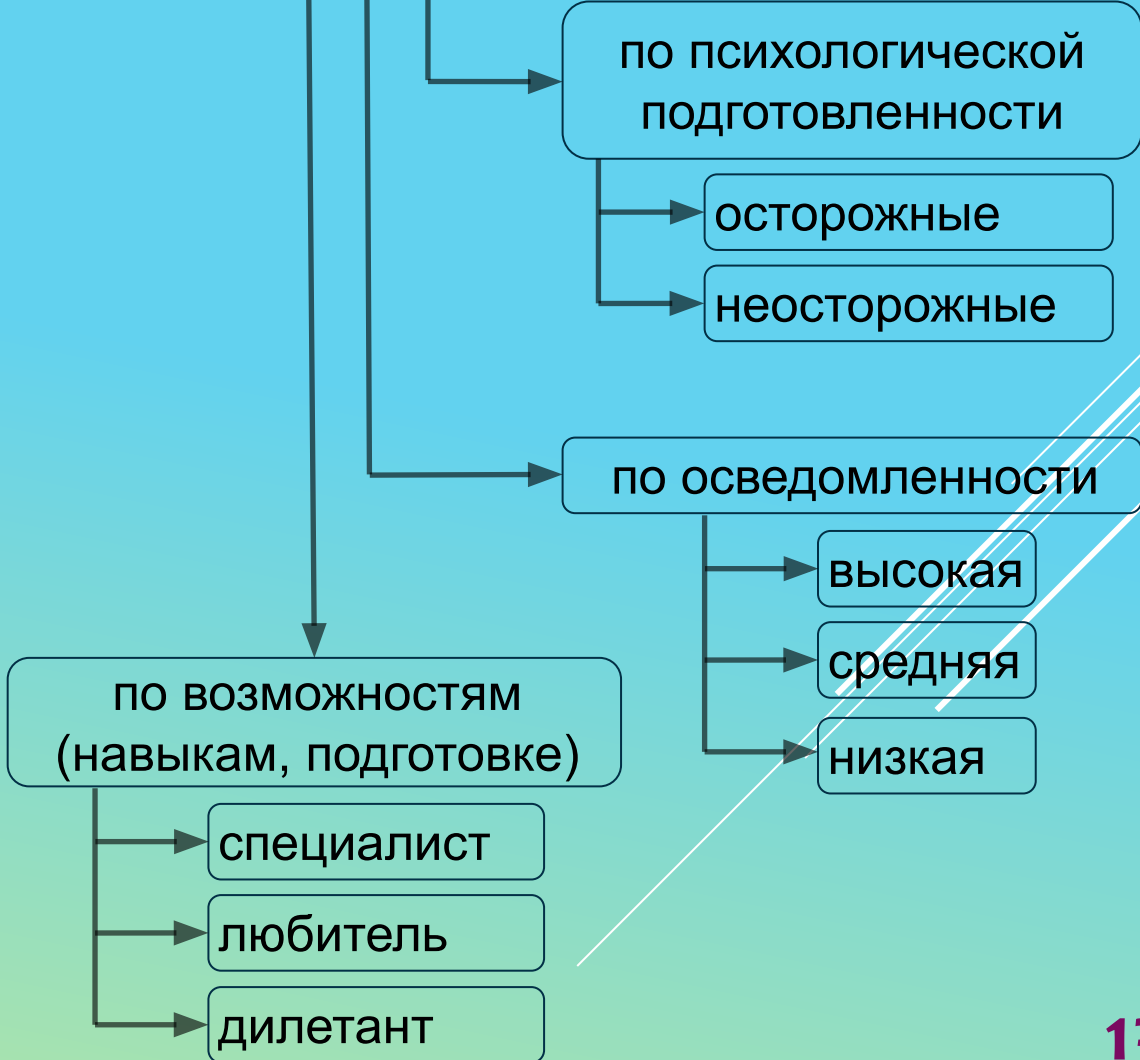
**Внутренние нарушители** - нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

**Внешние нарушители** - нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации.

# ВНУТРЕННИЕ НАРУШИТЕЛИ

## классификация внутренних нарушителей

- системные администраторы и администраторы безопасности
- авторизованные пользователи систем и сетей
- разработчики программных, программно-аппаратных средств
- поставщики услуг связи, вычислительных услуг
- лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ
- лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем оператора (администрация, охрана, уборщики и др.)



## Распространённые внутренние угрозы

- Удаление информации (часто при увольнении)
- Продажа информации с целью получения финансовой выгоды
- Похищение интеллектуальной собственности
- Опубликование конфиденциальной информации
- Рабочие места пользователей, подвергшиеся атаке вредоносного программного обеспечения (USB носители)
- Использование ресурсов организации в личных целях (майнинг)
- Отправка электронных писем не тому получателю
- Отсутствие настроек прав доступа к документам, размещённым в облачном хранилище
- Обработка информации на личных компьютерах

# ВНЕШНИЕ НАРУШИТЕЛИ

## классификация внешних нарушителей

- иностранные спецслужбы
- террористические, экстремистские и иные преступные группы
- отдельные физические лица (хакеры)
- лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем
- посетители / клиенты
- конкурирующие организации
- бывшие (уволенные) работники (пользователи)

### по осведомленности

- высокая
- средняя
- низкая

### по возможностям (навыкам, подготовке)

- новички (novice)
- подготовленные (learning)
- повседневные (casual)
- мастера (guru)

### **Возможности нарушителя зависят от:**

- ✓ состояние объекта защиты;
- ✓ наличие потенциальных каналов утечки информации;
- ✓ наличие средств защиты информации;
- ✓ качество средств защиты информации.

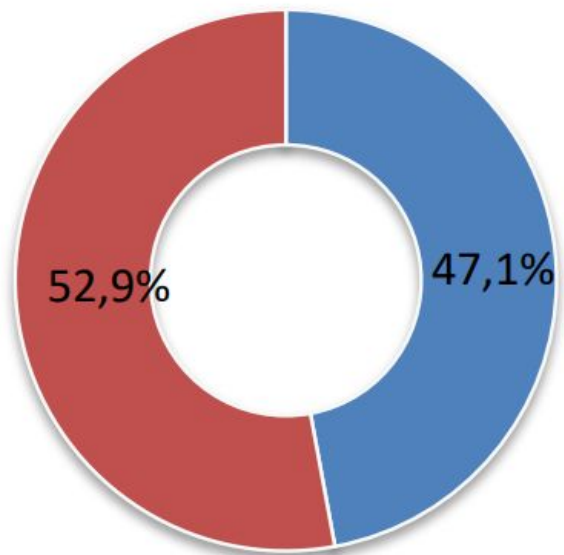
### **Мотивация (или зачем они это делают?):**

- ✓ неопытность;
- ✓ любопытство;
- ✓ безответственность (самоутверждение);
- ✓ корыстный интерес;
- ✓ угрозы и шантаж третьих лиц.



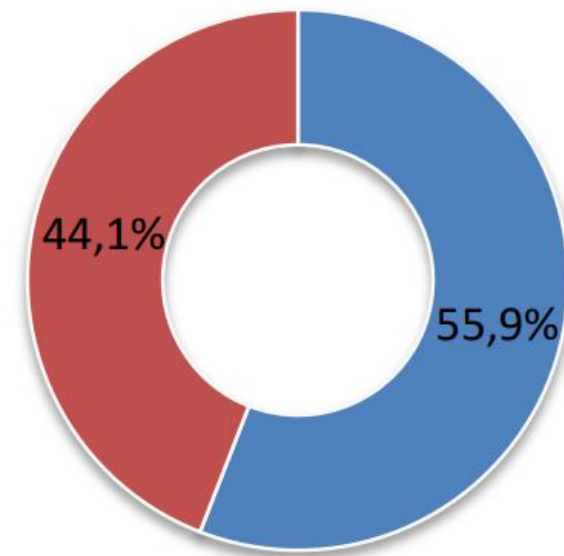
## РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО КАТЕГОРИИ НАРУШИТЕЛЕЙ 2019-2020 ГГ.\*

2019



- Внешний нарушитель
- Внутренний нарушитель

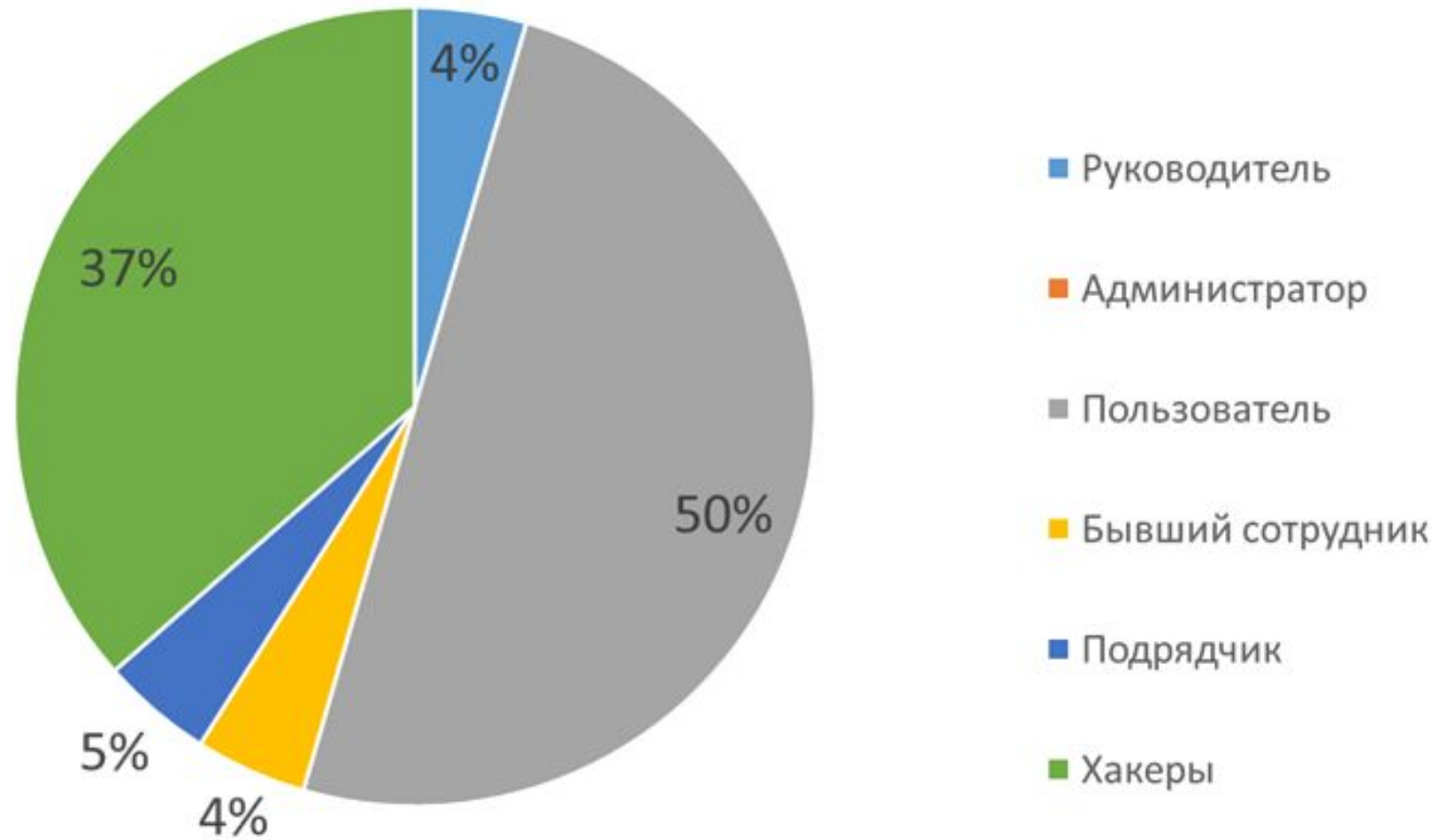
2020



- Внешний нарушитель
- Внутренний нарушитель

\* Источник: Исследование утечек информации ограниченного доступа // InfoWatch

## РАСПРЕДЕЛЕНИЕ УТЕЧЕК ПО ВИНОВНИКАМ НАРУШЕНИЙ



## МЕТОДЫ, ИСПОЛЬЗУЕМЫЕ ДЛЯ ПОЛУЧЕНИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

- Социальный инжиниринг
- Фишинг (вид социального инжиниринга)
- Эксплуатация уязвимостей
- Вредоносное ПО удаленного доступа
- Вирусы-вымогатели
- Флуд
- DDoS-атаки
- Backdoor
- Троян
- Руткит
- Фрод
- Brute force

## КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ



- Скриншоты экранов
- Фотографирование
- Копирование (печать) документов
- Мессенджеры
- Электронная почта
- Социальные сети
- Съёмные носители информации
- Облачные хранилища
- Удаленный доступ
- Мобильные устройства
- Сети передачи данных (проводные, беспроводные)
- Кража, утрата

## РАСПРЕДЕЛЕНИЕ КАНАЛОВ УТЕЧЕК ИНФОРМАЦИИ



# ТЕЗИСЫ

**БЕЗОПАСНОСТЬ ИНФОРМАЦИИ —  
ЭТО НЕ ТЕХНОЛОГИЧЕСКАЯ ПРОБЛЕМА,  
ЭТО ПРОБЛЕМА ЛЮДЕЙ И МЕНЕДЖМЕНТА.**

**СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ  
ДОЛЖНА ПОМОГАТЬ, А НЕ СРЫВАТЬ  
РЕАЛИЗАЦИЮ БИЗНЕС-ПРОЦЕССОВ**

## ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

- Организация охранных мероприятий
- Организация контроля доступа в помещения (серверные)
- Обеспечение физической безопасности вычислительных средств:
  - активные методы;
  - пассивные методы.
- Контроль выданных машинных носителей информации, вычислительных средств

## ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

- Разработка политики управления доступом
- Управление учетными записями
- Разграничение прав доступа
- Обеспечение информационного взаимодействия (маршрутизация, фильтрация, контроль зашифрованного трафика, диоды данных, физическое и логической разделение информационных потоков)
- Разделение обязанностей (контроль доступа / аудит / информационное взаимодействие)
- Ограничение привилегий (изменение системных настроек)
- Ограничение неудачных попыток входа (подбор пароля)
- Уведомление об используемой системе



## ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

- Уведомление о предыдущем входе в систему
- Ограничение одновременных сеансов
- Контроль подключаемых устройств
- Завершение сеанса (по времени, бездействию)
- Определение действий не требующих идентификации и аутентификации
- Автоматизированная маркировка информации (установка ассоциативных атрибутов)
- Контроль удаленного доступа
- Контроль беспроводного доступа
- Контроль доступа для мобильных устройств
- Контроль доступа к внешним системам
- Защита данных

## Статья 29. Меры по защите информации (Закон № 455-3)

**ПРАВОВЫЕ МЕРЫ** – заключаемые владельцем информации с пользователем информации договоры, в которых устанавливаются условия пользования информацией, а также ответственность сторон по договору за нарушение указанных условий.

**ОРГАНИЗАЦИОННЫЕ МЕРЫ** – обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации.

**ТЕХНИЧЕСКИЕ МЕРЫ** – меры по использованию средств **технической** и **криптографической** защиты информации, а также меры по контролю защищенности информации.

**Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196  
«О некоторых мерах по совершенствованию защиты информации»**

**Техническая защита информации** – деятельность, направленная на обеспечение **конфиденциальности, целостности, доступности и сохранности** информации.

**средства технической защиты информации** – **технические, программные, программно-аппаратные** средства, предназначенные для защиты информации от несанкционированного доступа и несанкционированных воздействий на нее, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности.

**Криптографическая защита информации** – деятельность, направленная на обеспечение **конфиденциальности, контроля целостности и подлинности** информации с использованием **средств криптографической защиты информации**.

**средства криптографической защиты информации** – **программные, программно-аппаратные** средства, реализующие один или несколько **криптографических алгоритмов** (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности.

**КОНФИДЕНЦИАЛЬНОСТЬ** – гарантия того, что сообщения доступны для понимания или использования только тем сторонам, которым они предназначены.

**ПОДЛИННОСТЬ** – гарантия того, что сторона действительно является владельцем, создателем или отправителем определенного сообщения.

**ЦЕЛОСТНОСТЬ** – гарантия того, что в сообщение не внесены изменения при его хранении, передаче и обработке.

**ДОСТУПНОСТЬ (информации, ресурсов информационной системы)** – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно (ГОСТ Р 50922-2006).

**ЦЕЛОСТНОСТЬ** – состояние защищенности информации, характеризующее способность автоматизированной системы обеспечивать сохранность и неизменность информации при попытках несанкционированных воздействий на нее в процессе обработки или хранения (ГОСТ Р 52863-2007).

## СРЕДСТВА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1	Средства защиты от воздействия вредоносных программ и антивирусные программные средства.
2	Маршрутизаторы и коммутаторы, выполняющие функцию маршрутизации.
3	Межсетевые экраны.
4	Системы сбора и обработки данных событий информационной безопасности.
5	Системы обнаружения и предотвращения вторжений.
6	Системы обнаружения и предотвращения утечек информации из информационных систем.

## СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1	Средства предварительного шифрования.
2	Средства линейного шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь.
3	Средства выработки электронной цифровой подписи.
4	Криптографические токены (программно-аппаратные средства ЭЦП).
5	Средства проверки электронной цифровой подписи.
6	Средства выработки личного ключа или открытого ключа.
7	Терминал взаимодействия с криптографическим токеном.
8	Регистрационный центр.
9	Терминал взаимодействия с криптографическим токеном.
10	Клиентская программа для взаимодействия с криптографическим токеном.
11	Средства контроля целостности.

## ТРЕБОВАНИЯ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

Технический регламент Республики Беларусь  
«Информационные технологии. Средства защиты информации.  
Информационная безопасность»  
(ТР 2013/027/ВУ)  
(утвержден постановлением  
Совета Министров Республики Беларусь  
от 15 мая 2013 г. № 375  
с изменениями и дополнениями от 12 марта 2020 г. № 145).

Перечень государственных стандартов,  
взаимосвязанных с техническим регламентом Республики Беларусь  
«Информационные технологии. Средства защиты информации.  
Информационная безопасность»  
(ТР 2013/027/ВУ)  
(утвержден приказом Оперативно-аналитического центра при  
Президенте Республики Беларусь от 12 марта 2020 г. № 77  
в редакции приказа Оперативно-аналитического центра при  
Президенте Республики Беларусь от 28 декабря 2022 г. № 207).

УТВЕРЖДЕНО

Приказ  
Оперативно-аналитического  
центра при Президенте  
Республики Беларусь  
12.03.2020 № 77

(в редакции приказа  
Оперативно-аналитического  
центра при Президенте  
Республики Беларусь  
28.12.2022 №207)

### ПЕРЕЧЕНЬ

государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ)

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
1.	Генераторы электромагнитного шума	СТБ 1875-2011 «Средства защиты информации. Генераторы электромагнитного шума. Общие технические требования и методы испытаний» (пункты 5.1.1, 5.1.2.2, 5.1.2.5, 5.1.2.10, 5.1.2.11, 5.1.2.15, 5.1.3)	
2.	Фильтры помехоподавляющие	СТБ 1966-2012 «Средства защиты информации. Фильтры помехоподавляющие. Общие технические требования и методы испытаний» (пункты 4.1.1.4 – 4.1.1.6, 4.1.4.3)	
3.	Генераторы линейного зашумления	СТБ 2256-2012 «Средства защиты информации. Генераторы линейного зашумления. Общие технические требования и методы испытаний» (пункты 4.1.1, 4.1.2.2, 4.1.2.5, 4.1.2.7, 4.1.2.8, 4.1.2.10, 4.1.3.1)	
4.	Фильтры-ограничители	СТБ 2296-2012 «Средства защиты информации. Фильтры-ограничители. Общие технические требования и методы испытаний» (пункты 4.1.1.1, 4.1.1.2)	
5.	Средства защиты речевой информации от утечки по акустическому и виброакустическому каналам	СТБ 34.101.28-2011 «Информационные технологии. Средства защиты речевой информации от утечки по акустическому и виброакустическому каналам. Общие технические требования» (пункты 4.2, 4.3.1, 4.3.2, 4.3.5 – 4.3.10)	
6.	Средства контроля защищенности речевой информации	СТБ 34.101.29-2011 «Информационные технологии. Средства контроля защищенности речевой информации. Общие технические требования» (пункт 4.2)	
7.	Средства защиты речевой информации от утечки	СТБ 2352-2013 «Информационные технологии. Средства защиты речевой информации от утечки по каналам	



№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
	по каналам высокочастотного навязывания	высокочастотного навязывания. Общие технические требования и методы испытаний» (пункты 4.3.2 – 4.3.4, 4.7.1.1 – 4.7.1.4, 4.7.2.1, 4.7.2.2)	
8.	Средства пассивной технической защиты цифровых телефонных аппаратов от утечки речевой информации по каналам акустоэлектрического преобразования и высокочастотного навязывания	СТБ 34.101.84-2019 «Информационные технологии. Средства пассивной технической защиты цифровых телефонных аппаратов от утечки речевой информации по каналам акустоэлектрического преобразования и высокочастотного навязывания в двухпроводной цифровой линии связи. Общие технические требования и методы испытаний» (пункты 5.3.3 – 5.3.5, 5.3.7, 5.4.6, 5.5)	
9.	Средства защиты от воздействия вредоносных программ и антивирусные программные средства	СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования» (пункты 6.2 и (или) 6.3, и (или) 6.4, и (или) 6.5, и (или) 6.6, и (или) 6.7, и (или) 6.8, и (или) 6.9)	
10.	Маршрутизаторы и коммутаторы, выполняющие функцию маршрутизации	СТБ 34.101.14-2017 «Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования»	
11.	Операционные системы для использования на автоматизированных рабочих местах органов государственного управления при обработке государственных секретов	СТБ 34.101.51-2011 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы для использования на автоматизированных рабочих местах органов государственного управления при обработке государственных секретов»	Номенклатура контролируемых показателей должна быть определена в задании по безопасности на производство, разработанном в соответствии с профилем защиты
12.	Межсетевые экраны	СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) 7.6)	
13.	Системы сбора и обработки данных событий информационной безопасности	СТБ 34.101.74-2017 «Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования» (пункты 7.2 и (или) 7.3)	
14.	Системы обнаружения и предотвращения вторжений	СТБ 34.101.75-2017 «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5, и (или) 7.6, и (или) 7.7, и (или) 7.8, и (или) 7.9)	
15.	Системы обнаружения и предотвращения утечек информации из информационных систем	СТБ 34.101.76-2017 «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем.	

№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
		Общие требования» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.5)	
16.	Средства предварительного шифрования	<p>СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности» (пункты 7.2 и (или) 7.3, и (или) 7.4, и (или) 7.9, и (или) 7.10)</p> <p>СТБ 34.101.31 (пункт 7.6 схема 1 и (или) 2), и (или) СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции» (пункт 8.13)</p> <p>СТБ 34.101.31 (пункт 7.5) и (или) СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел» (пункт 6.1)</p> <p>СТБ 34.101.27-2022 «Информационные технологии и безопасность. Средства криптографической защиты информации. Требования безопасности» (пункт 5.10) и (или) СТБ 34.101.47 (пункты 6.2, и (или) 6.3)</p> <p>СТБ 34.101.31 (пункты 7.8 и (или) 8.1, и (или) 8.2), и (или) СТБ 34.101.77 (раздел 7, и (или) пункт 8.12), и (или) СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых» (пункт 6.1)</p> <p>СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых» (пункт 7.2)</p> <p>СТБ 34.101.66 (пункты 7.4 и (или) 7.5, и (или) 7.6)</p> <p>СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей» (разделы 6, 7, 8), СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»</p>	<p>Требования к криптографическим алгоритмам (обязательно должен быть реализован один из алгоритмов шифрования) Алгоритмы шифрования</p> <p>Алгоритмы аутентифицированного шифрования</p> <p>Обязательно при обеспечении контроля целостности (алгоритмы имитозащиты)</p> <p>Требования к криптографическим протоколам и управлению криптографическими ключами</p> <p>Требования к генерации случайных (псевдослучайных) чисел</p> <p>Обязательно при предварительном распределении криптографических ключей</p> <p>Обязательно при транспорте криптографических ключей</p> <p>Обязательно при согласовании общего криптографического ключа</p> <p>Обязательно при распространении открытых ключей в виде сертификатов открытых ключей</p>



№ п/п	Наименование средств защиты информации	Обозначение и наименование государственного стандарта (применяемые требования)	Примечание
		СТБ 34.101.27 (пункт 5.11)	защиты информации
		СТБ 34.101.27 (пункт 5.12)	Обязательно при наличии в составе средств криптографической защиты информации компонентов или комплексов с открытыми исходными текстами программ
		СТБ 34.101.27 (пункт 6.3)	Обязательно при хранении в пределах криптографической границы криптографических ключей в незашифрованном виде
		СТБ 34.101.23 (раздел 8), СТБ 34.101.78 (пункт 8.6)	Обязательно при наличии удаленного доступа к средству криптографической защиты информации
		СТБ 34.101.23 (раздел 9), СТБ 34.101.78 (пункт 8.7)	Требования к форматам Требования к подписанным данным Требования к конвертованным данным
24.	Иные программные, программно-аппаратные средства защиты информации	СТБ 34.101.1-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель», СТБ 34.101.2-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности», СТБ 34.101.3-2014 «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности»	В качестве основы для оценки средств защиты информации используется задание по безопасности



Мероприятия **по технической и криптографической защите информации**, осуществляемые организациями, должны предусматривать:

- ✓ в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено - обеспечение **конфиденциальности, целостности и подлинности** информации;
- ✓ в информационных системах, в которых обрабатываются электронные документы - обеспечение **целостности и подлинности** данных документов.



### Общедоступная информация.

Требования по защите общедоступной информации **могут** устанавливаться только в целях **недопущения** ее **уничтожения, модификации (изменения), блокирования правомерного доступа к ней.**

Защита сведений, составляющих **государственные секреты** – Закон Республики Беларусь от 19.07.2010 № 170-З «О государственных секретах».



### Информация, распространение и (или) предоставление которой ограничено.

Информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам, должна обрабатываться в информационных системах с применением **системы защиты информации, аттестованной** в порядке, установленном Оперативно-аналитическим центром при Президенте Республики Беларусь.

Для создания **системы защиты информации** используются средства **технической и криптографической** защиты информации, имеющие **сертификат соответствия**, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или **положительное экспертное заключение** по результатам государственной экспертизы, порядок проведения которой определяется Оперативно-

Не допускается эксплуатация государственных информационных систем без реализации мер по защите информации.

**Приказ Оперативно-аналитического центра  
при Президенте Республики Беларусь  
от 20 февраля 2020 г. № 66**

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

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

Положение о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации.

Положение о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации.

Положение о порядке ведения Государственного реестра критически важных объектов информатизации.

**Комплекс мероприятий по технической и криптографической защите информации включает:**

- ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ
- СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ
- АТТЕСТАЦИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ
- ОБЕСПЕЧЕНИЕ ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ
- ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В СЛУЧАЕ ПРЕКРАЩЕНИЯ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

До проведения работ по проектированию системы защиты информации **собственник (владелец)** информационной системы **осуществляет категорирование информации**, которая будет обрабатываться в информационной системе, с оформлением «Акта отнесения информационной системы к классу типовых информационных систем».

## **КЛАССЫ типовых информационных систем. Общедоступная информация.**

**6-частн** – негосударственные информационные системы, в которых обрабатывается **общедоступная информация** (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных.

**6-гос** – государственные информационные системы, в которых обрабатывается **общедоступная информация** (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных.

**5-частн** – негосударственные информационные системы, в которых обрабатывается **общедоступная информация** (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных.

**5-гос** – государственные информационные системы, в которых обрабатывается **общедоступная информация** (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных.

# КЛАССЫ типовых информационных систем.

## Информация, распространение и (или) предоставление которой ограничено.

**4-ин** – информационные системы, в которых обрабатываются **персональные данные**, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

**4-спец** – информационные системы, в которых обрабатываются **специальные персональные данные**, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

**4-бг** – информационные системы, в которых обрабатываются **биометрические и генетические персональные данные** и которые не имеют подключений к открытым каналам передачи данных.

**4-юл** – информационные системы, в которых обрабатывается **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), и которые не имеют подключений к открытым каналам передачи данных.

**4-дсп** – информационные системы, в которых обрабатывается **служебная информация ограниченного распространения** и которые не имеют подключений к открытым каналам передачи данных.

**3-ин** – информационные системы, в которых обрабатываются **персональные данные**, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.

**3-спец** – информационные системы, в которых обрабатываются **специальные персональные данные**, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных.

**3-бг** – информационные системы, в которых обрабатываются **биометрические и генетические персональные данные** и которые подключены к открытым каналам передачи данных.

**3-юл** – информационные системы, в которых обрабатывается **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), и которые подключены к открытым каналам передачи данных.

**3-дсп** – информационные системы, в которых обрабатывается **служебная информация ограниченного распространения** и которые подключены к открытым каналам передачи данных.

На этапе проектирования системы защиты информации осуществляются:

- ✓ 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;
- ✓ издание политики информационной безопасности. При этом физическое лицо, являющееся собственником (владельцем) информационной системы, в которой обрабатываются персональные данные, за исключением индивидуального предпринимателя, вправе не издавать политику информационной безопасности;
- ✓ определение требований к системе защиты информации **в техническом задании** на создание системы защиты информации (далее – техническое задание);
- ✓ выбор средств **технической** и **криптографической** защиты информации;
- ✓ разработка (корректировка) общей схемы системы защиты информации.

## Техническое задание на систему защиты информации должно содержать:

- требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3;

- требования к средствам криптографической защиты информации, включая требования к криптографическим алгоритмам в зависимости от задач

4-ин	установлены для следующих классов типовых информационных систем безопасности (шифрование, выработка и проверка электронной цифровой подписи, хэширование, и др. для защиты), криптографическим протоколам, 3-ин
1	управлению криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям
2	безопасности и форматам данных. Профили требований, предъявляемых к средствам криптографической защиты информации, определяются
3	Требования по обеспечению идентификации и аутентификации Оперативно-аналитическим центром при Президенте Республики Беларусь;
4	□ Требования к защите систем защиты информации информационной системы
5	Обеспечение криптографической защиты информации
6	Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре
7	Иные требования



Приложение 3  
к Положению о порядке технической  
и криптографической защиты информации  
в информационных системах, предназначенных  
для обработки информации, распространение  
и (или) предоставление которой ограничено  
(в редакции приказа  
Оперативно-аналитического  
центра при Президенте  
Республики Беларусь  
12.11.2021 № 195)

**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	+/-	+/-	+	+/-	+/-	+	+	+	+	+/-	+									
1.4	Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
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	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2	Требования по обеспечению защиты данных																				
2.1	Регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2.2	Обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, сетевого оборудования, системного программного обеспечения и средств защиты информации	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
2.3	Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого оборудования, системного	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+



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 информационную систему. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
7.17	Обеспечение обнаружения и предотвращения вторжений в информационную систему 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	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+	+	+
7.19	Определение перечня внешних подключений к информационной системе и порядка такого подключения	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
7.20	Обеспечение контроля за внешними подключениями к информационной системе	+/-	+/-	+/-	+/-	+/-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
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	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+	+/-	+	+/-	+	+	+	+	+	+	+

Примечания:  
1. Обозначения «4-ин», «4-спец», «4-бг», «4-юл», «4-дсп», «3-ин», «3-спец», «3-бг», «3-юл» и «3-дсп» соответствуют классам типовых информационных систем.  
2. Требования, отмеченные знаком «+», являются обязательными.  
3. Требования, отмеченные знаком «+/-», являются рекомендуемыми.

## Техническое задание на систему защиты информации должно содержать:

- требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3;
- 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 Техническим регламентом Республики Беларусь (ТР 2013/027(Вед) Оперативным (Постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375);
- перечень документации на систему защиты информации.

Перечень государственных стандартов,  
взаимосвязанных с техническим регламентом Республики Беларусь  
(Приказ Оперативно-аналитического центра при Президенте Республики Беларусь  
от 28 декабря 2022 г. № 207).

## Техническое задание на систему защиты информации должно содержать:

- требования к системе защиты информации в зависимости от используемых технологий
- Документация на систему защиты информации должна содержать перечень параметров, подлежащих резервированию и уничтожению информации;
- требования к средствам криптографической защиты информации, включая требования к криптографическим алгоритмам в зависимости от задач использования съемных носителей информации;
- использования электронной почты (подписи, хэширование, имитозащита), криптографическим протоколам, управления криптографическими ключами (генерация, распределение, хранение, доступ, уничтожение), а также к функциональным возможностям осуществления контроля (мониторинга) за функционированием информационной системы и системы защиты информации, предъявляемых к средствам криптографической защиты информации, определяются
- реагирования на события информационной безопасности и ликвидации их последствий;
- оперативно-аналитическим центром при Президенте Республики Беларусь;
- перечень документации на систему защиты информации.
- управления криптографическими ключами, в том числе требования по их генерации, распределению, хранению, доступу к ним и их уничтожению.

Организационные меры по криптографической защите информации должны включать в себя меры по обеспечению особого режима допуска на территорию (в помещения), на которой может быть осуществлен доступ к средствам криптографической защиты информации и криптографическим ключам (носителям), а также по разграничению доступа к ним по кругу лиц.

Работы могут выполняться:

- ✓ **подразделением защиты информации** или иным подразделением (должностным лицом) **собственника (владельца)** информационной системы, ответственным за обеспечение защиты информации;
- ✓ **организациями, имеющими специальные разрешения (лицензии)** на деятельность по технической и (или) криптографической защите информации.

Мероприятия **по технической и криптографической защите информации**, осуществляемые организациями, должны предусматривать:

- ✓ в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено - обеспечение **конфиденциальности, целостности** и **подлинности** информации;
- ✓ в информационных системах, в которых обрабатываются электронные документы - обеспечение **целостности** и **подлинности** данных документов.

**Электронный документ** - документ в электронном виде с реквизитами, позволяющими установить его **целостность** и **подлинность**, которые подтверждаются путем применения **сертифицированных средств электронной цифровой подписи** с использованием при проверке электронной цифровой подписи открытых ключей организации или физического лица (лиц), подписавших этот электронный документ.

Электронный документ состоит из двух неотъемлемых частей - общей и особенной.

**Общая часть** электронного документа состоит из информации, составляющей содержание документа.

**Особенная часть** электронного документа состоит из одной или нескольких электронных цифровых подписей.

Особенная часть электронного документа может содержать *штамп времени*, а также *дополнительные данные*, необходимые для проверки электронной цифровой подписи (электронных цифровых подписей) и идентификации электронного документа, которые устанавливаются техническими нормативными правовыми актами.

**Электронная цифровая подпись** - последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его **целостности** и **подлинности**, а также для иных целей.

**Электронная цифровая подпись** предназначена для:

- удостоверения информации, составляющей общую часть электронного документа;
- подтверждения **целостности** и **подлинности** электронного документа;
- подписания электронной копии документа на бумажном носителе;
- иных целей, предусмотренных Законом Республики Беларусь «Об электронном документе и электронной цифровой подписи» и иными законодательными актами Республики Беларусь.

**Электронная цифровая подпись**, владельцем личного ключа которой является организация, может применяться:

- в качестве аналога оттиска печати организации;
- совместно с электронной цифровой подписью, владельцем личного ключа которой является физическое лицо, если информация о полномочиях этого физического лица, предоставленных ему от имени этой организации, не содержится в атрибутом сертификате;
- для создания и (или) подписания электронных документов посредством автоматизированных информационных систем без участия физического лица;
- в иных случаях, предусмотренных законодательством Республики Беларусь.

**Подлинность электронного документа** – свойство электронного документа, определяющее, что электронный документ подписан действительной электронной цифровой подписью (электронными цифровыми подписями).

**Целостность электронного документа** – свойство электронного документа, определяющее, что в электронный документ не были внесены изменения.

**Электронная копия документа на бумажном носителе** – электронное отображение документа на бумажном носителе, соответствующее оригиналу и подписанной электронной цифровой подписью лица, изготовившего такое электронное отображение.

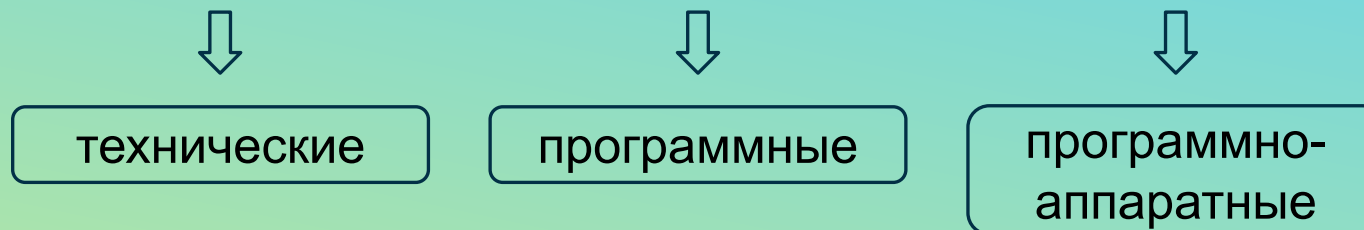


# СРЕДСТВА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

**Техническая защита информации** – деятельность, направленная на обеспечение **конфиденциальности, целостности, доступности** и **сохранности** информации.

**средства технической защиты информации** – **технические, программные, программно-аппаратные** средства, предназначенные для защиты информации от несанкционированного доступа и несанкционированных воздействий на нее, блокирования правомерного доступа к ней, иных неправомерных воздействий на информацию, а также для контроля ее защищенности.

**Средства технической защиты информации делятся на:**



## **СРЕДСТВА ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ**

- 1 Средства защиты от воздействия вредоносных программ и антивирусные программные средства.
- 2 Маршрутизаторы и коммутаторы, выполняющие функцию маршрутизации.
- 3 Межсетевые экраны.
- 4 Системы сбора и обработки данных событий информационной безопасности.
- 5 Системы обнаружения и предотвращения вторжений.
- 6 Системы обнаружения и предотвращения утечек информации из информационных систем.

## ТЕХНИЧЕСКИЕ НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ

Средства защиты от воздействия вредоносных программ и антивирусные программные средства:

**СТБ 34.101.8-2006** «Информационные технологии. Методы и средства безопасности. Программные и программно-аппаратные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования»

Маршрутизаторы и коммутаторы, выполняющие функцию маршрутизации:

**СТБ 34.101.14-2017** «Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования»

Межсетевые экраны:

**СТБ 34.101.73-2017** «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования»

**Системы сбора и обработки данных событий информационной безопасности:**

**СТБ 34.101.74-2017** «Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования»

**Системы обнаружения и предотвращения вторжений:**

**СТБ 34.101.75-2017** «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования»

**Системы обнаружения и предотвращения утечек информации из информационных систем:**

**СТБ 34.101.76-2017** «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования»

## Иные программные, программно-аппаратные средства защиты информации:

В качестве основы для оценки средств защиты информации используется задание по безопасности.

**СТБ 34.101.1-2014** «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»

**СТБ 34.101.2-2014** «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности»

**СТБ 34.101.3-2014** «Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности»

# СОБЫТИЕ

идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

## МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

- ✓ настройка критериев отбора событий из системных журналов штатных средств (идентификаторы пользователей, дата, время, и подробности событий, отчеты об успешных и отклоненных событиях);
- ✓ получение событий из системных журналов штатных средств;
- ✓ сборы системных журналов с активного сетевого оборудования;
- ✓ сохранение полученных событий и системных журналов;
- ✓ выборка событий безопасности по заданным критериями;
- ✓ регистрация сбоев, о которых сообщают пользователи;
- ✓ оповещение о событиях безопасности;
- ✓ просмотр событий безопасности;
- ✓ проведение анализа событий безопасности;
- ✓ синхронизация системного времени.



## РАСПРОСТРАНЕННЫЕ СОБЫТИЯ БЕЗОПАСНОСТИ, КОТОРЫЕ РЕКОМЕНДУЕТСЯ АНАЛИЗИРОВАТЬ

- Создание учетных записей
- Изменение прав доступа для пользователей
- Изменения в системных настройках
- Изменение настроек безопасности
- Удачные и неудачные попытки входа
- Несанкционированная установка программного обеспечения
- Повышение входящего или исходящего трафика
- Изменение конфигураций оборудования
- Изменение правил межсетевого экрана
- Изменение в таблицах базы данных
- Выгрузка конфиденциальной информации из базы данных
- Удаленный доступ



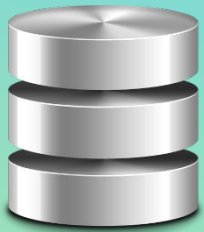
Авторизация:  
как успешная,  
так и неуспешная



Срабатывания  
антивирусного ПО,  
IDS\IPS, DLP, СЗИ



Бесконтрольный выход  
в Internet и соцсети



Подозрительные  
запросы к СУБД,  
аномальные нагрузки  
на СУБД



Нетипичное  
поведение  
пользователя



Удаленный доступ

## ИСТОЧНИКИ СОБЫТИЙ БЕЗОПАСНОСТИ

**Журналы событий серверов и рабочих станций** (контроль доступа, обеспечения непрерывности, соблюдения политик информационной безопасности)

**Access Control, Authentication** (мониторинг контроля доступа и использования привилегий)

**Антивирусные приложения** (события о работоспособности ПО, базах данных, изменении конфигураций и политик, вредоносном коде)

**Межсетевые экраны** (сведения об атаках, вредоносном ПО и прочем)

**Сетевое активное оборудование** (контроль доступа, учет сетевого трафика)

**Сканеры уязвимостей** (данные об инвентаризации активов, сервисов, программного обеспечения, уязвимостей, поставка инвентаризационных данных и топологической структуры)

**Системы инвентаризации (asset-management)** (данные для контроля активов в инфраструктуре и выявления новых)

**Системы веб-фильтрации** (данные о посещении сотрудниками подозрительных или запрещенных веб-сайтов)

**DLP-системы** (работает внутри контура на утечки, попытки инсайдерских утечек, нарушения прав доступа)

**IDS/IPS-системы** (реагирует на воздействия на контур извне, данные о сетевых атаках, изменениях конфигурации и доступа к устройствам)

# СБОР ЛОГОВ ДЛЯ ЦЕНТРАЛИЗОВАННОГО ВЕДЕНИЯ ЖУРНАЛА

## OPEN SOURCE решения

**ELK**

**FLUENTD (KUBERNETES)**

**GRAYLOG**

**LOGPACKER**

**LOGWATCH**

**LNAV (LOG FILE  
NAVIGATOR)**

**SIEM (Security information and event management, «управление событиями и информацией о безопасности»)** - класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.

В задачи SIEM-систем входит:

- ✓ в реальном времени отслеживать сигналы тревоги, поступающие от сетевых устройств и приложений;
- ✓ обрабатывать полученные данные и находить взаимосвязи между ними;
- ✓ выявлять отклонения от нормального поведения контролируемых систем;
- ✓ оповещать операторов об обнаруженных инцидентах.

SIEM-системы только собирают и обрабатывают данные, а также оповещают оператора о возможной опасности. Блокирование подозрительных процессов, помещение файлов на карантин и прочие меры реагирования в их задачи не входят.

## SIEM-системы

- ✓ программное средство "**IBM Security Qradar SIEM**";
- ✓ программный комплекс "Система управления событиями безопасности "**RuSIEM**";
- ✓ программный комплекс "Система мониторинга и управления событиями безопасности "**FortSIEM**";
- ✓ программный комплекс "Система мониторинга и управления событиями безопасности "**Ankey SIEM**";
- ✓ программный комплекс сбора и обработки данных событий информационной безопасности "**Bytis SIEM**";
- ✓ программное обеспечение "**LibraSIEM**";
- ✓ программное изделие "Система мониторинга событий информационной безопасности "**MaxPatrol SIEM**".

## **DLP-СИСТЕМЫ**

*(DATA LEAK PREVENTION)*

### **СИСТЕМЫ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ ИЗ ИНФОРМАЦИОННЫХ СИСТЕМ**

- Технологии предотвращения утечек информации из информационной системы вовне, а также технические устройства (программные или программно-аппаратные) для предотвращения утечек.
- Строятся на анализе потоков данных, пересекающих периметр защищаемой информационной системы. При детектировании в этом потоке конфиденциальной информации срабатывает активная компонента системы, и передача сообщения (пакета, потока, сессии) блокируется.

#### **Уровни контроля DLP-системы:**

1. **уровень сети** – контролируется сетевой трафик в информационной системе (**невозможно контролировать зашифрованный трафик**);
2. **уровень хоста** – контролируется информация на рабочих станциях, полный контроль за действиями пользователя (**недостаток: потребление ресурсов рабочей станции**).

## ОСНОВНЫЕ ФУНКЦИИ DLP УРОВНЯ СЕТИ

- Администрирование
- Мониторинг сетевых соединений
- Фильтрация данных
- Анализ графических и текстовых файлов
- Анализ видео и аудио файлов
- Анализ файлов по их форматам или содержимому
- Маркировка обнаруженных инцидентов (блокировка, карантин, оповещение, перенаправление)
- Реакция на обнаруженные инциденты (блокировка, перенаправление, карантин)
- Поддержка национальных кодировок
- Регистрация событий в журнале аудита
- Обновление базы правил
- Восстановление после сбоев



## ОСНОВНЫЕ ФУНКЦИИ DLP УРОВНЯ ХОСТА

- Администрирование
- Контроль записи защищаемой информации
- Контроль вывода на печать защищаемой информации на локальные принтеры
- Контроль вывода на печать защищаемой информации на сетевые принтеры
- Контроль операций пользователя с буфером обмена
- Блокирование возможности несанкционированного перемещения и клонирования защищаемой информации
- Наличие механизмов контроля защищаемой информации
- Регистрация событий в журнале аудита
- Восстановление после сбоев

## РАСПРОСТРАНЁННЫЕ ОШИБКИ НАСТРОЙКИ DLP

- Реализация шаблонных правил (настройка с учетом бизнес-процессов)
- Охват не всех возможных каналов утечки конфиденциальных данных
- Ложные инциденты, которые администратор-ИБ не успевает обработать вручную (настройка по умолчанию обрачивается лавиной оповещений)
- Неспособность предупредить утечку данных (необходимо настройка с учетом деятельности сотрудников)
- Ухудшение эффективности DLP в связи с выстраиванием информационных потоков вокруг системы
- Не учтены юридические аспекты (правовое обеспечение функционирования системы)

## DLP-системы

- ✓ программное обеспечение "**LibraDLP**";
- ✓ программный комплекс "**Teramind DLP**";
- ✓ программный комплекс "**Гарда Предприятие**";
- ✓ программный комплекс "**Broadcom Data Loss Enterprise Suite**";
- ✓ программный комплекс "**InfoWatch Traffic Monitor**";
- ✓ программный комплекс "Система контроля защищенности и соответствия стандартам **MaxPatrol**";
- ✓ программное изделие "**Forcepoint DLP**";
- ✓ программное обеспечение "**Falcongaze SecureTower**".

# IDS/IPS-СИСТЕМЫ

**IDS** (Intrusion Detection System) - система обнаружения вторжений.

**IPS** (Intrusion Prevention System) - система предотвращения вторжений.

Используются для защиты от сетевых атак. Основное различие между ними в том, что **IDS** - это система мониторинга, а **IPS** - система управления. По сравнению с традиционными средствами защиты - антивирусами, спам-фильтрами, файерволами - **IDS/IPS** обеспечивают гораздо более высокий уровень защиты сети.

# IDS

## Виды IDS:

- ✓ уровень сети (Network Intrusion Detection System - **NIDS**);
- ✓ уровень хоста (Host-based Intrusion Detection System - **HIDS**).

## Принцип действия IDS:

- ✓ сигнатурные;
- ✓ аномальные (статистические, аномалии протокола и трафика);
- ✓ основанные на правилах.

## Задачи IDS:

- ✓ обнаружение и регистрация атак;
- ✓ оповещение при срабатывании определенного правила.

## IDS умеют выявлять:

- ✓ различные виды сетевых атак;
- ✓ обнаруживать попытки неавторизованного доступа;
- ✓ повышение привилегий;
- ✓ появление вредоносного ПО;
- ✓ отслеживать открытие нового порта и т. д.

# IPS

## **IPS устанавливается:**

- ✓ «в разрыв», работает на втором уровне модели OSI, не имеет IP-адреса (mas), а значит остается невидимой для взломщика;
- ✓ на зеркалируемый трафик.

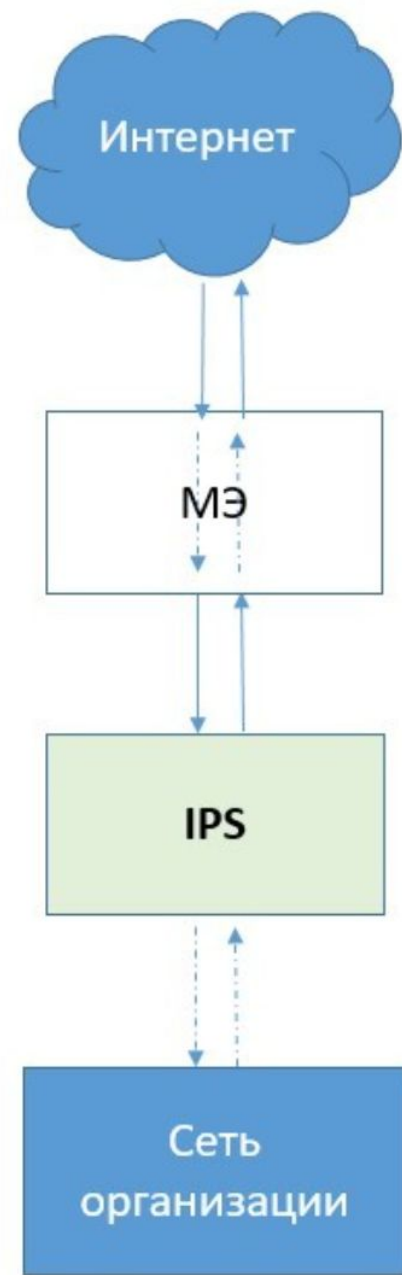
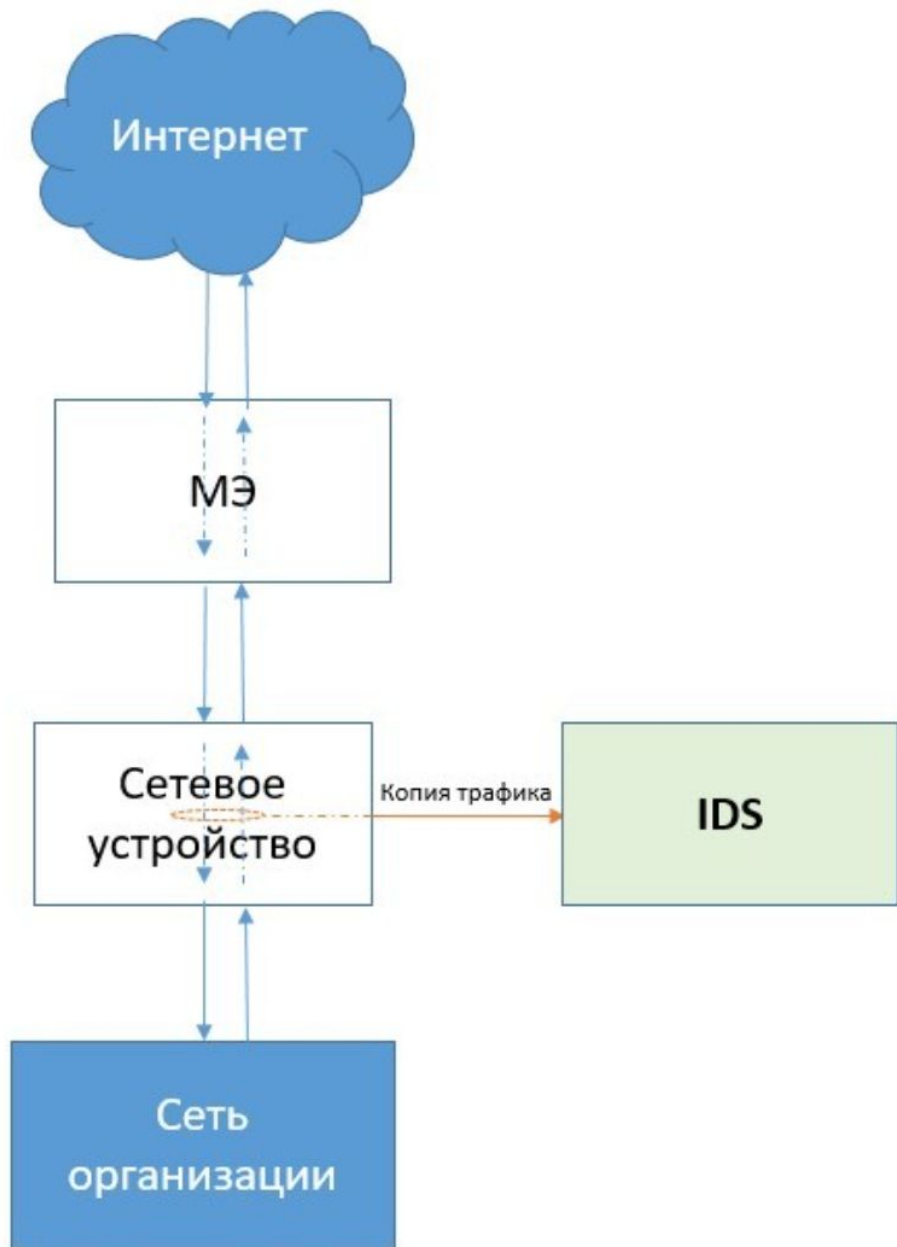
## **IPS защищает:**

- ✓ локальную систему от вирусов;
- ✓ руткитов (набор утилит для скрытия следов пребывания);
- ✓ взлома и т.д.

## **IDS помечает трафик:**

- ✓ пропустить (pass);
- ✓ уведомление или тревога (alert);
- ✓ отбросить (drop);
- ✓ отклонить (reject).

IDS-система не отражает атаки, а всего лишь обнаруживает и помечает все подозрительные действия, а заблокировать атакующий хост в реальном времени помогает IPS.



## РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ IDS/IPS

- Систему необходимо разворачивать на входе защищаемой сети или подсети и обычно за межсетевым экраном.
- Перед активацией функции **IPS** следует некоторое время погонять систему в режиме, не блокирующем, **IDS**. В дальнейшем потребуется периодически корректировать правила.
- Большинство настроек **IPS** установлены с расчетом на типичные сети. В определённых случаях они могут оказаться неэффективными, поэтому необходимо обязательно указать IP внутренних подсетей и используемые приложения (порты).
- Если **IPS**-система устанавливается «в разрыв», необходимо контролировать ее работоспособность, иначе выход устройства из строя может запросто парализовать всю сеть.



## АНТИВИРУС. СОСТАВНЫЕ МОДУЛИ

- ✓ **антивирусный сканер** — утилита, выполняющая поиск вредоносных программ на дисках и в памяти устройства по запросу пользователя или по расписанию;
- ✓ **резидентный монитор** — компонент, выполняющий отслеживание состояния системы в режиме реального времени и блокирующий попытки загрузки или запуска вредоносных программ на защищаемом компьютере;
- ✓ **брандмауэр (firewall)** — компонент, выполняющий мониторинг текущего соединения, включая анализ входящего и исходящего трафика, а также проверяющий исходный адрес и адрес назначения в каждом передаваемом с компьютера и поступающем на компьютер пакете информации - данные, поступающие из внешней среды на защищенный брандмауэром компьютер без предварительного запроса, отслеживаются и фильтруются. С функциональной точки зрения брандмауэр выступает в роли своеобразного фильтра, контролирующего поток передаваемой между локальным компьютером и интернетом информации, защитного барьера между компьютером и всем остальным информационным пространством;

- ✓ **веб-антивирус** — компонент, предотвращающий доступ пользователя к опасным ресурсам, распространяющим вредоносное ПО, фишинговым и мошенническим сайтам с использованием специальной базы данных адресов или системы рейтингов;
- ✓ **почтовый антивирус** — приложение, выполняющее проверку на безопасность вложений в сообщения электронной почты и (или) пересылаемых по электронной почте ссылок;
- ✓ **модуль антируткит** — модуль, предназначенный для борьбы с руткитами (вредоносными программами, обладающими способностью скрывать свое присутствие в инфицированной системе);
- ✓ **модуль превентивной защиты** — компонент, обеспечивающий целостность жизненно важных для работоспособности системы данных и предотвращающий опасные действия программ;
- ✓ **модуль обновления** — компонент, обеспечивающий своевременное обновление других модулей антивируса и вирусных баз;
- ✓ **карантин** — централизованное защищенное хранилище, в которое помещаются подозрительные (в некоторых случаях - определенно инфицированные) файлы и приложения до того, как по ним будет вынесен окончательный вердикт.

## МЕТОДЫ ОБНАРУЖЕНИЯ ВРЕДНОСНЫХ ПРОГРАММ

- **Сигнатурное детектирование** (создании уникальных цифровых идентификаторов файла).
- **Поведенческий анализ** (антивирусная программа следит за поведением приложений).
- **Эвристический анализ** (антивирус загружает подозрительное приложение в собственную буферную память, разбирает код на инструкции).
- **Проактивная защита HIPS** (Host-based Intrusion Prevention) (Антивирус следит за запущенными приложениями и информирует пользователя о тех или иных действиях программы).

## МЕТОДЫ ПРОТИВОДЕЙСТВИЯ АНТИВИРУСАМ

- **Переупаковка** - программные упаковщики сжимают содержимое файла приложения и дописывают к нему код, необходимый для распаковки и выполнения программы тем самым изменяют сигнатуру файла;
- **Обфускация** (от англ. obfuscate – «запутывать», «сбивать с толку») – приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции;
- **Антиотладка** – вредоносное программное обеспечение анализирует работающие процессы и сравнивает их с заданным списком, ищет что оно не запущено в песочнице или в режиме отладки.

# СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

**Криптографическая защита информации** – деятельность, направленная на обеспечение **конфиденциальности**, контроля **целостности** и **подлинности** информации с использованием **средств криптографической защиты информации**.

**средства криптографической защиты информации** – **программные, программно-аппаратные** средства, реализующие один или несколько **криптографических алгоритмов** (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами и функциональные возможности безопасности.

## Средства криптографической защиты информации делятся на:



### программные:

- уровень 1 (базовый);
- уровень 2 (средний).



### программно-аппаратные:

- уровень 3 (высокий);
- уровень 4 (максимальный).

## Криптографические алгоритмы делятся на:

- **Алгоритмы с секретным ключом (симметричные)** используются в средствах линейного и предварительного шифрования для обеспечения конфиденциальности и контроля целостности.
- **Алгоритмы с открытым ключом (асимметричные)** используются в средствах электронной цифровой подписи для обеспечения подлинности и целостности электронного документа.
- **Бесключевые алгоритмы** (алгоритмы хэширования, алгоритмы разделения секрета, алгоритмы построения семейства ключей) используются для обеспечения контроля целостности, защиты объектов и создания и модификации ключей.

# СИММЕТРИЧНЫЕ АЛГОРИТМЫ

## **СТБ 34.101.31-2020 Алгоритмы шифрования и контроля целостности**

- 1) belt-ecb алгоритм шифрования в режиме простой замены;
- 2) belt-cbc алгоритм шифрования в режиме сцепления блоков;
- 3) belt-cfb алгоритм шифрования в режиме гаммирования с обратной связью;
- 4) belt-ctr алгоритмы шифрования в режиме счетчика;
- 5) belt-mac алгоритм выработки имитовставки;
- 6) belt-dwp алгоритм аутентифицированного шифрования данных;
- 7) belt-kwp алгоритм аутентифицированного шифрования ключа;
- 8) belt-dbe дискового шифрования, алгоритм блочного шифрования;
- 9) belt-sde дискового шифрования, алгоритм секторного шифрования;
- 10) belt-fmt алгоритм шифрования с сохранением формата.

## **СТБ 34.101.77-2020 Криптографические алгоритмы на основе sponge-функции**

- 1) bash-prng-ae алгоритм аутентифицированного шифрования.



# АССИМЕТРИЧНЫЕ АЛГОРИТМЫ

## СТБ 34.101.45-2013 Алгоритм электронной цифровой подписи и транспорта ключа на основе эллиптических кривых

- 1) Алгоритм выработки и проверки электронной цифровой подписи;  
(уровень стойкости – 128: bign-with-hbelt; 192: bign-with-bash384; 256: bign-with-bash512)
- 2) Алгоритм транспорта ключа  
**Средства электронной цифровой подписи** – средство защиты информации, с помощью которого реализуется подписание информации

## СТБ 34.101.66-2014 Протоколы формирования общего ключа на основе эллиптических кривых

- ✓ 1) **Протокол Диффи-Хеллмана** (bake-dh);  
выработка электронной цифровой подписи;
- ✓ **A** и **B** обмениваются параметрами эллиптической кривой
- проверка электронной цифровой подписи;
- **A** и **B** генерируют личные ключи и вычисляют открытые  $Q_a = d_a G$  и  $Q_b = d_b G$
- ✓ выработка личного ключа или открытого ключа.
- **A** и **B** обмениваются открытыми ключами (проверяют что полученные ключи являются элементом группы точек)
- **A** определяет точку  $K = d_a Q_b$ , а **B**  $K = d_b Q_a$
- **Транспорт ключа** – конфиденциальная передача ключа от одной стороны другой.
- по точке **K** стороны строят общий ключ

- 2) BMQV (bake-bmqv);
- 3) BSTS (bake-bsts);
- 4) BPACE (bake-pace).

## СТБ 34.101.79-2019 Криптографические токены

- 1) BAUTH (btok-bauth).

## БЕСКЛЮЧЕВЫЕ АЛГОРИТМЫ

### **СТБ 34.101.31-2020 Алгоритмы шифрования и контроля целостности**

- 1) belt-hash алгоритм хэширования (выходными данными является хэш = 256 bit);
- 2) belt-keyexpand алгоритм расширения ключа;
- 3) belt-keyrep алгоритм преобразования ключа;
- 4) алгоритм разделения секрета.

### **СТБ 34.101.77-2020 Криптографические алгоритмы на основе sponge-функции**

- 1) bash-hash (L) – выходными данными является хэш  $2L$ , где L уровень стойкости (128, 192, 256).

## СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- 1 Средства предварительного шифрования.
- 2 Средства линейного шифрования, в том числе для использования в системах профессиональной радиосвязи Республики Беларусь.
- 3 Средства выработки электронной цифровой подписи.
- 4 Криптографические токены (программно-аппаратные средства ЭЦП).
- 5 Средства проверки электронной цифровой подписи.
- 6 Средства выработки личного ключа или открытого ключа.
- 7 Терминал взаимодействия с криптографическим токеном.
- 8 Регистрационный центр.
- 9 Терминал взаимодействия с криптографическим токеном.
- 10 Клиентская программа для взаимодействия с криптографическим токеном.
- 11 Средства контроля целостности.

## ПЕРЕЧЕНЬ ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ, ПОДЛЕЖАЩИХ ВКЛЮЧЕНИЮ В ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Установлены для следующих классов типовых информационных систем

4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп	3-ин
1	Аудит безопасности									
2	Требования по обеспечению защиты данных									
3	Требования по обеспечению идентификации и аутентификации									
4	Требования по защите системы защиты информации информационной системы									
5	<b>Обеспечение криптографической защиты информации</b>									
6	Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре									
7	Иные требования									

## ПЕРЕЧЕНЬ ТРЕБОВАНИЙ К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ, ПОДЛЕЖАЩИХ ВКЛЮЧЕНИЮ В ТЕХНИЧЕСКОЕ ЗАДАНИЕ

5	Обеспечение криптографической защиты информации	4-ин	4-спец	4-бг	4-юл	4-дсп	3-ин	3-спец	3-бг	3-юл	3-дсп
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)	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-	+/-

## СРЕДСТВА ПРЕДВАРИТЕЛЬНОГО ШИФРОВАНИЯ

**Предварительное шифрование** – способ шифрования, при котором зашифрование и расшифрование данных разнесено по времени с процессом их передачи (приема) по каналу связи.

### Способы управления криптографическими ключами:

- ✓ предварительное распределение ключей;
- ✓ транспорт ключа;
- ✓ согласование ключа;
- ✓ пароль (не используется в СКЗИ).

## СРЕДСТВА ЛИНЕЙНОГО ШИФРОВАНИЯ

**Линейное шифрование** – способ шифрования, при котором зашифрование и расшифрование данных производится непосредственно в процессе передачи (приема) по линиям электросвязи, без возможности промежуточного хранения.

### **Способы управления криптографическими ключами:**

- ✓ предварительное распределение ключей;
- ✓ открыто распределенные ключи.

Протоколы безопасной передачи данных приложений:

- **TLS** (протокол защиты транспортного уровня) [ [RFC8446](#) ] — это распространенный протокол, используемый для установления безопасного сеанса между двумя конечными точками (TLS 1.2, TLS 1.3)
- **DTLS** (безопасность транспортного уровня дейтаграмм) [ [RFC6347](#) ] [ [DTLS-1.3](#) ] основан на TLS, но отличается тем, что он предназначен для работы с ненадежными протоколами дейтаграмм, такими как UDP.
- **Security RTP (SRTP)** — это профиль для RTP, который обеспечивает конфиденциальность, аутентификацию сообщений и защиту от воспроизведения для пакетов данных RTP и пакетов протокола управления RTP (RTCP) [ [RFC3711](#) ].



## TLS (TRANSPORT LAYER SECURITY PROTOCOL)

**СТБ 34.101.65-2014** Информационные технологии и безопасность. Протокол защиты транспортного уровня **TLS** (Transport Layer Security Protocol).

Обеспечивает аутентификацию сторон протокола, **конфиденциальность** и контроль **целостности** передаваемой информации.

Объединяет несколько субпротоколов, разбитых на два уровня:

**Транспортный уровень:**

протокол **Record** (**конфиденциальность** и контроль **целостности**).

**Прикладной уровень**, протоколы:

**Handshake** (аутентификация сторон и согласования общих ключей);

**Change Cipher Spec** (смена параметров защиты);

**Alert** (извещение о закрытии сессии и ошибках).

- **Ipsec** IKEv2 [ [RFC7296](#) ] и ESP [ [RFC4303](#) ] вместе образуют современный набор протоколов IPsec, который шифрует и аутентифицирует IP-пакеты.
- WireGuard [ [WireGuard](#) ] — это протокол IP-уровня, разработанный как альтернатива IPsec для определенных случаев использования. В отличие от большинства протоколов безопасности транспорта, используя предварительно общие открытые ключи, доставляемые вне диапазона, каждый из которых привязан к одному или нескольким IP-адресам. Более того, как протокол, подходящий для VPN, WireGuard не предлагает возможности расширения, согласования или криптографической гибкости.
- **OpenVPN** [ [OpenVPN](#) ] — широко используемый протокол, разработанный как альтернатива IPsec.

## ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ (PKI – Public Key Infrastructure)

**Государственная система управления открытыми ключами (ГосСУОК)** предназначена для обеспечения возможности получения всеми заинтересованными организациями и физическими лицами информации об открытых ключах и их владельцах в Республике Беларусь и представляет собой систему взаимосвязанных и аккредитованных в ней поставщиков услуг.

Строится как иерархическая инфраструктура открытых ключей и состоит из корневого удостоверяющего центра, подчиненного ему республиканского удостоверяющего центра и регистрационных центров.

Сертификаты открытых ключей, изданные в **ГосСУОК**, обязательны к применению при обращении электронных документов во всех государственных информационных системах, а также в иных информационных системах, содержащих информацию, распространение и (или) предоставление которой ограничено.

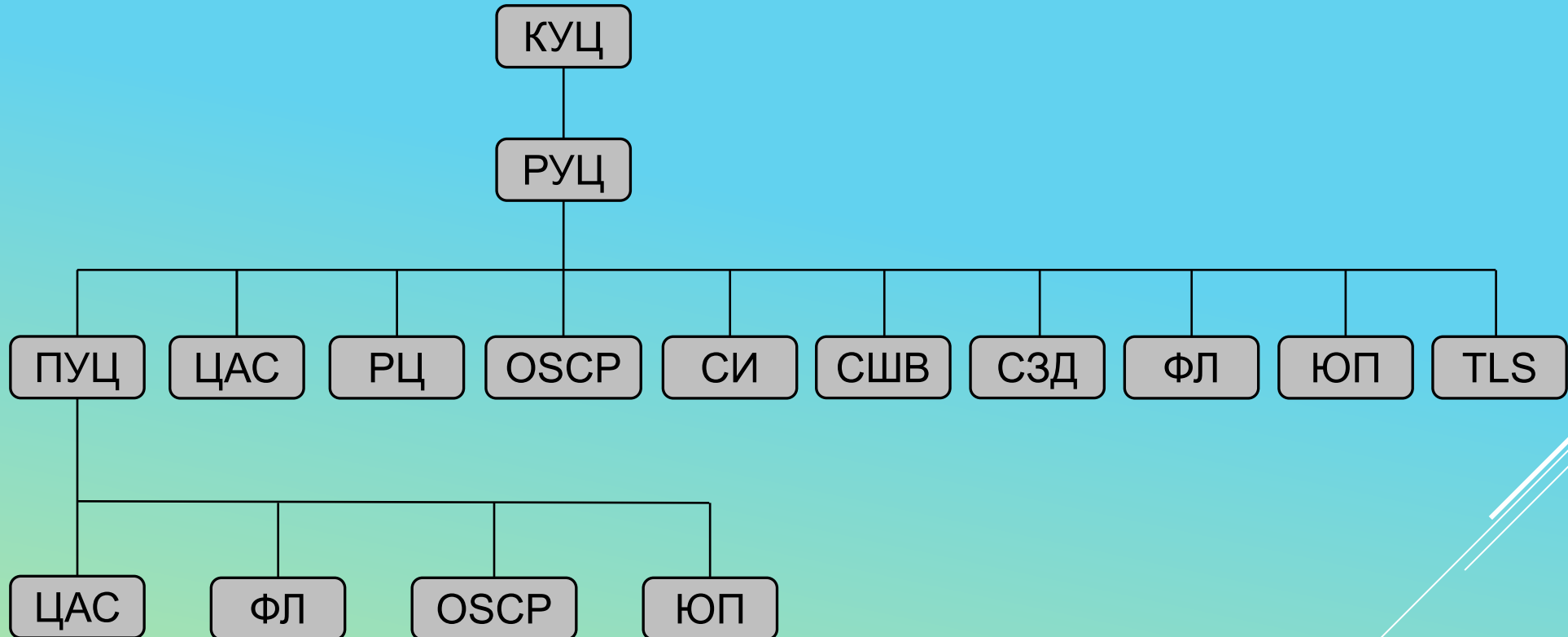
Распространение открытых ключей государственных органов и других государственных организаций, атрибутивных сертификатов физических лиц, работающих в таких органах и организациях, осуществляется через Государственную систему управления открытыми ключами.

## Основные функции ГосСУОК

- ✓ регистрация владельцев личных ключей;
- ✓ издание, распространение и хранение сертификатов открытых ключей, атрибутивных сертификатов, списков отозванных сертификатов открытых ключей и списков отозванных атрибутивных сертификатов;
- ✓ предоставление информации о действительности сертификатов открытых ключей, атрибутивных сертификатов;
- ✓ проставление штампа времени;
- ✓ создание и сопровождение баз данных действующих и отозванных сертификатов открытых ключей, атрибутивных сертификатов;
- ✓ внесение сертификатов открытых ключей, атрибутивных сертификатов в базы данных действующих сертификатов открытых ключей, атрибутивных сертификатов;
- ✓ обеспечение доступности баз данных действующих и отозванных сертификатов открытых ключей, атрибутивных сертификатов;
- ✓ отзыв сертификатов открытых ключей, атрибутивных сертификатов;
- ✓ достоверное подтверждение принадлежности открытого ключа определенным организациям или физическому лицу.

# ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

## СТОРОНЫ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ



# ИНФРАСТРУКТУРА ОТКРЫТЫХ КЛЮЧЕЙ

**КУЦ** (корневой удостоверяющий центр)

**РУЦ** (республиканский удостоверяющий центр)

**ЦАС** (центр атрибутивных сертификатов). Подчиняется РУЦ либо одному из ПУЦ. Выпускает атрибутивные сертификаты для конечных участников.

**РЦ** (регистрационный центр). Подчиняется РУЦ. проводит первичную аутентификацию, регистрирует идентификационные данные, организует подготовку запросов на получение сертификата, визирует запросы.

**OCSP-сервер**. Подчиняется РУЦ либо одному из ПУЦ. По запросам сторон выпускает справки (OCSP-ответы) о текущем статусе сертификатов.

**СШВ** (служба штампов времени). Подчиняется РУЦ. По запросам сторон выпускает штампы времени, которые демонстрируют существование определенных данных к определенному моменту времени.

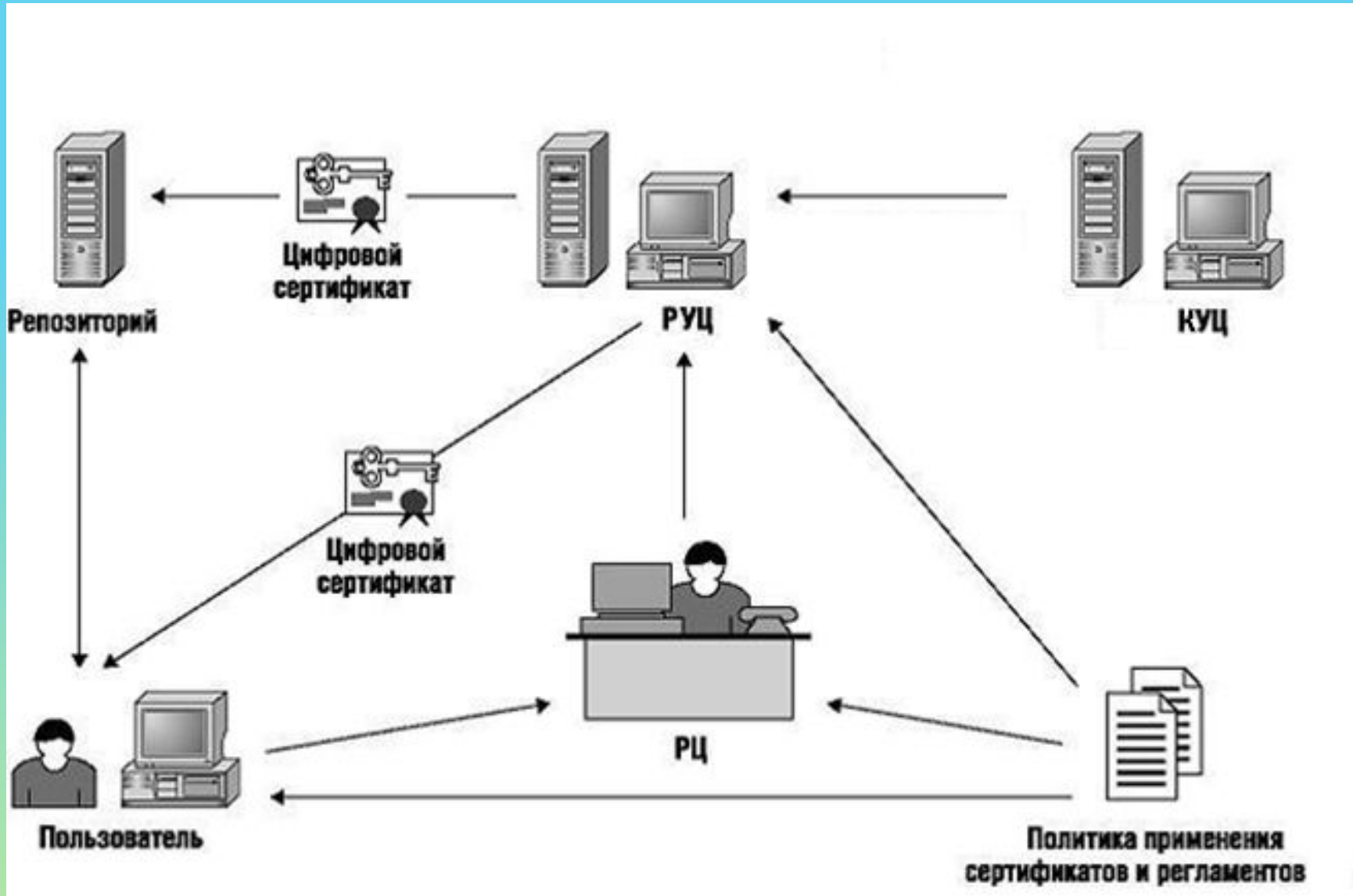
**СЗД** (служба заверения данных). Подчиняется РУЦ. По запросам сторон выпускает справки (аттестаты заверения) о действительности ЭД.

**СИ** (служба идентификации). Подчиняется РУЦ либо одному из ПУЦ. Проводит аутентификацию пользователей и, в случае успеха, выдает билеты.

**TLS-сервер**. Подчиняется РУЦ. Является частью прикладной системы, организует ее взаимодействие с другими сторонами по защищенным TLS-соединениям.

**ФЛ** (физическое лицо). Получает сертификат в РУЦ либо в одном из ПУЦ. Может быть как резидентом, так и нерезидентом Республики Беларусь.

**ЮП** (юридический представитель). Получает сертификат в РУЦ либо в одном из ПУЦ. Представляет ЮЛ, несет ответственность за выполнение определенных процессов: технологических, юридических, организационных, финансовых и пр.





# ИНФРАСТРУКТУРА КРИПТОГРАФИЧЕСКИХ ТОКЕНОВ

- КРИПТОГРАФИЧЕСКИЙ ТОКЕН
- КЛИЕНТСКАЯ ПРОГРАММА
- ТЕРМИНАЛ

**Криптографический токен** – СКЗИ имеющее конкретного владельца и выступающее от его лица при взаимодействии с другими сторонами.

В состав криптографического токена входят прикладные программы:

**eID** – предназначена для управления идентификационными данными владельца токена.

**eSign** – предназначена для генерации личных и открытых ключей, выработку электронной цифровой подписи и разбора токена ключа.

Криптографический токен используется в двух режимах:

- 1) **Базовый** (не требует онлайн взаимодействия с другими сторонами).
- 2) **Терминальный** (взаимодействие с прикладными системами онлайн).

**БИОМЕТРИЧЕСКИЙ ДОКУМЕНТ,  
УДОСТОВЕРЯЮЩИЙ ЛИЧНОСТЬ,  
ИДЕНТИФИКАЦИОННАЯ КАРТА**

Средство криптографической защиты информации  
“Карта пластиковая идентификационная с интегральной микросхемой”  
(ТУ ВУ 100093319.012-2020), сертификат соответствия  
№ ВУ/112 02.01 ТР027 036.01 00164, дата регистрации 25.08.2021 г.

## Java Card Applets

### eID:

DG1: ИД номер  
DG2: Данные КТ  
DG3: ФИО  
DG4: Дата рождения  
DG5: Пол

### eSign:

Name  
Attribute  
СОК(В)  
Хэш ОК(В)  
СОК(Т)  
Хэш ОК(Т)

### SecretKey:

KeyPRNG  
PrivateKeyAuth  
PIN1  
PIN2  
PUK  
CAN  
PrivateKey(В)  
PrivateKey(Т)

**MF:** Сведения о КТ  
Объект безопасности  
СОК ЭЦП от объекта безопасности  
Цепочка сертификатов для DS

JCOP4 P71 OS

**SecureBox:**  
NativeLib  
(с национальными криптографическими алгоритмами)



## КЛИЕНТСКАЯ ПРОГРАММА

- Организует взаимодействие КТ с владельцем и терминалом с использованием APDU команд
- Обрабатывает критические данные (PIN/PUC)
- Вычисляет хэш-значения подписываемых данных
- Обеспечивает выполнение протокола WPASE
- Обеспечивает создание защищенного соединения между КТ и КП

## ТЕРМИНАЛ

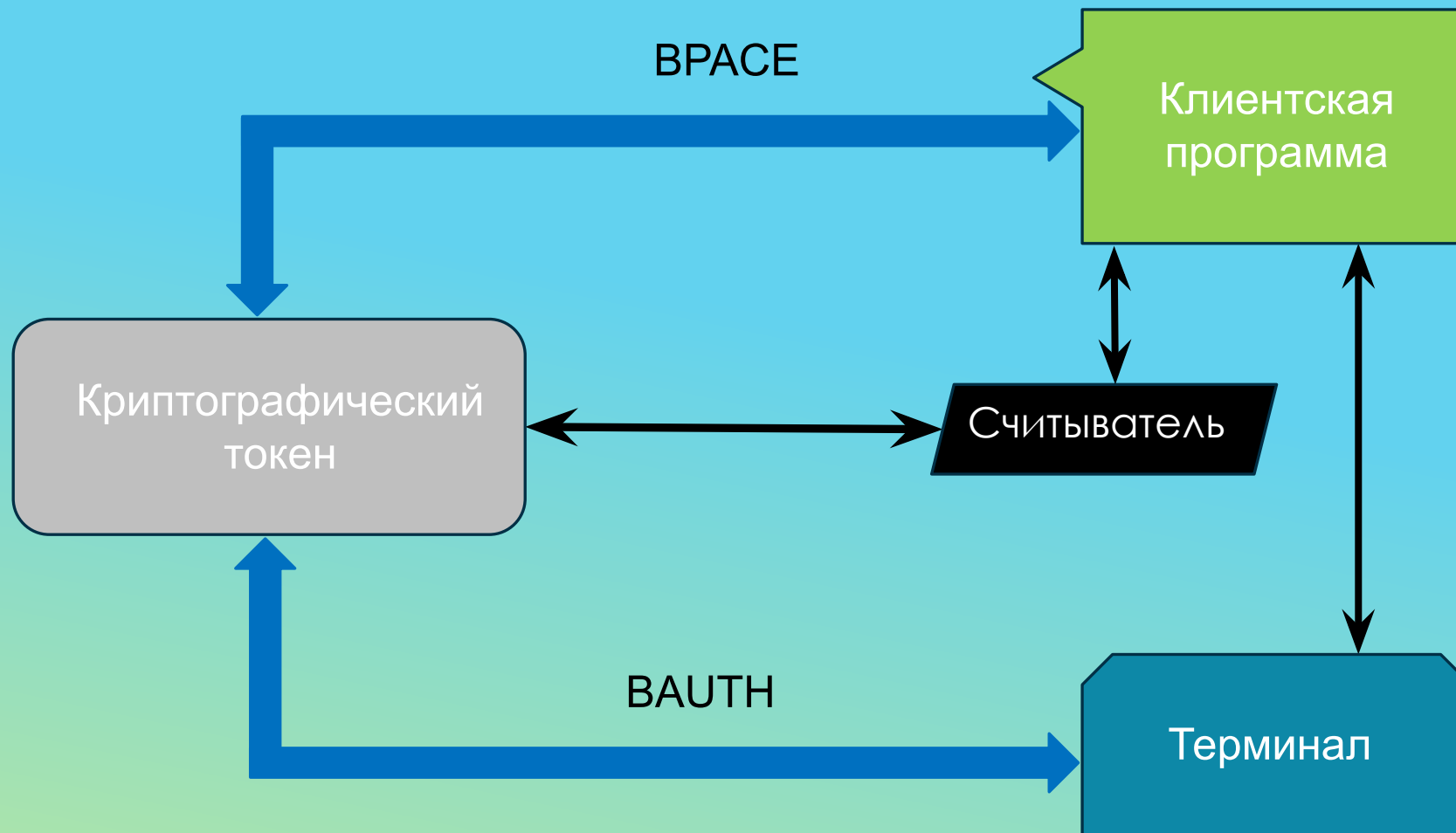
По исполнению бывают двух типов:

- ✓ **локальный** – взаимодействуют непосредственно с КТ (включает в себя КП и должен иметь аппаратное исполнение);
- ✓ **удаленный** – взаимодействует с КТ посредством сетей электросвязи при этом посредником является КП.

**Криптографическая поддержка:**

- ✓ протокол BAUTH;
- ✓ создание защищённого соединения.

## СТРУКТУРНАЯ СХЕМА ВЗАИМОДЕЙСТВИЯ



## СРЕДСТВА КОНТРОЛЯ ЦЕЛОСТНОСТИ

Средства контроля целостности предназначены для выявления изменений в передаваемой или хранимой информации по сравнению с ее исходной записью.

Делятся на следующие типы:

1. Использующие функции хэширования;
2. Использующие алгоритмы имитовставки;
3. Использующие алгоритм электронной цифровой подписи.

- ❑ При осуществлении технической и криптографической защиты информации используются средства технической и криптографической защиты информации, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.
- ❑ Криптографическая защита служебной информации ограниченного распространения осуществляется только с применением программно-аппаратных средств криптографической защиты информации.
- ❑ Особенности криптографической защиты информации в информационных системах, в которых обрабатываются электронные документы, могут устанавливаться законодательством об электронном документе и электронной цифровой подписи.





# ОПЕРАТИВНО-АНАЛИТИЧЕСКИЙ ЦЕНТР ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ



Информация об ОАЦ



Право



Новости



Деятельность ОАЦ в сфере защиты информации



Безопасный Интернет



Лотерейная деятельность и электронные интерактивные игры



Борьба с мошенничеством на сетях электросвязи



Обращения граждан и юридических лиц

## Реестр средств защиты информации, прошедших сертификацию

Перечень сертифицированных продуктов информационных технологий

[Скачать документ](#)

### Параметры

Поиск...

ГОСТ 28147-89

- раздел 2
- раздел 3
- раздел 4
- раздел 5

Оценка Задания по безопасности

Оценка продуктов информационных технологий

Оценка профиля защиты

СТБ 1176.1-99

СТБ 1176.2-99

- пункт 5.1
- пункт 6.1
- пункт 7.1
- раздел 5
- раздел 6
- раздел 7

СТБ 1875-2011

- 5.1.1
- 5.1.1.1
- 5.1.1.3
- 5.1.1.4

### Средства защиты информации

#### Программное средство канального шифрования "itVPN" (РБ.МЕЯШ.03007-02), серийное производство

Заявитель

Общество с ограниченной ответственностью "ИТТАС"

Адрес заявителя

Республика Беларусь, 220029, г.Минск, пр-т Машерова, д.15, этаж 2

Дополнительная информация (особые отметки)

Контрольные характеристики файлов в соответствии с Приложением

Регистрационный номер сертификата соответствия (экспертного заключения)  
ВУ/112 02.01. ТР027 036.01 00641

Дата внесения в реестр  
2022-12-30

Срок действия сертификата соответствия (экспертного заключения)  
2027-12-29

[Подробнее](#)

#### Комплекс программный криптографической защиты информации под управлением ОС Linux "БАС-L" ВУ.СЮИК.00450-01, серийное производство

Заявитель

Закрытое акционерное общество "НТЦ КОНТАКТ"

Адрес заявителя

Республика Беларусь, 220007, г.Минск, пер.Студенческий, д.7, пом.1

Дополнительная информация (особые отметки)

Контрольные характеристики файлов в соответствии с Приложением на одном листе (бланк МТБ №2753275)

Регистрационный номер сертификата соответствия (экспертного заключения)  
ВУ/112 02.01. ТР027 036.01 00640

Дата внесения в реестр  
2022-12-30

Срок действия сертификата соответствия (экспертного заключения)  
2027-12-29

[Подробнее](#)

**БЛАГОДАРЮ ЗА ВНИМАНИЕ!**

The image features a background with a vertical gradient from light blue at the top to light green at the bottom. In the center, the text "БЛАГОДАРЮ ЗА ВНИМАНИЕ!" is written in a bold, dark blue, sans-serif font. In the bottom right corner, there are several white, parallel diagonal lines that create a sense of motion or a modern design element.