ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ В УЧРЕЖДЕНИИ ОБРАЗОВАНИЯ

КАЦУБА В.Ю.,
начальник учебно-методического отдела
информационных технологий и издательской деятельности
it@iro.gomel.by

“Масштабная цифровизация, о которой правительство говорит годами, пока буксует. Статус IT-страны предполагает создание продукта для нужд собственной экономики в первую очередь. Для этого давались преференции. Отдачи пока не очень видно.”

Президент Республики Беларусь А.Г.Лукашенко

Доступность Интернета для белорусов

Согласно «Глобальному инновационному индексу 2024», опубликованному Всемирной организацией интеллектуальной собственности, **Беларусь заняла 22-е место среди 133-х государств по показателю «Доступ к ИКТ»**

The most important global business risks for 2026

Ranking changes are determined by positions year-on-year, ahead of percentages.

The 15th annual **Allianz Risk Barometer** survey was conducted among Allianz customers (global businesses), brokers and industry trade organizations. It also surveyed risk consultants, underwriters, senior managers and claims experts in the corporate insurance segment of Allianz Commercial and other Allianz entities.

View the full Allianz Risk Barometer 2026 rankings here

Rank		Percent	2025 rank	Trend
11	Critical infrastructure blackouts *(e.g., power disruption)* or failures *(e.g., aging dams, bridges, rail tracks)*[2]	8%	*12 (9%)*	↗
12	Talent or labor issues	8%	*11 (9%)*	↘
13	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	6%	*13 (8%)*	→
14	Theft, fraud, corruption[3]	5%	*14 (7%)*	→
15	Insolvency	5%	*16 (6%)*	↗
16	Loss of reputation or brand value *(e.g., public criticism)*[4]	4%	*15 (7%)*	↘
17	Biodiversity and nature risks *(e.g., water scarcity)*[5]	4%	NEW	↗
18	Product recall, quality management, serial defects	4%	*18 (4%)*	→
19	Human health risk *(e.g., pandemic outbreak)*	3%	*19 (3%)*	→
20	Pollution event	1%	*17 (6%)*	↘
	Other	2%		

Source: Allianz Commercial

Figures represent the number of risks selected as a percentage of all survey responses from 3,338 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.

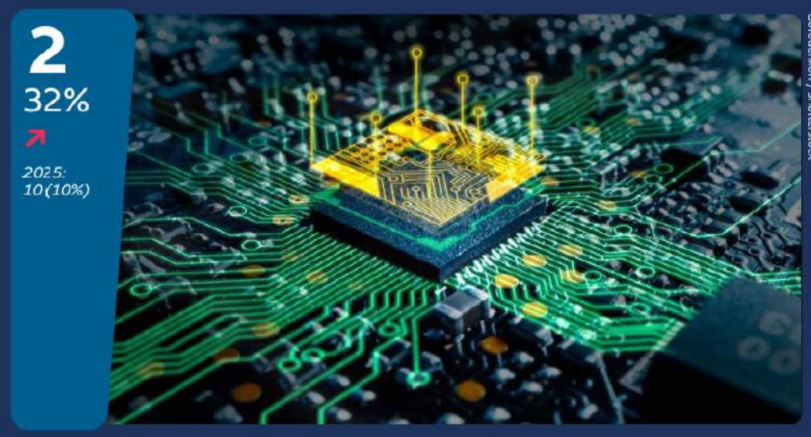
NEW New entry in the top risks

1 42% → *2025: 1 (38%)*

ImageFlow / Shutterstock

Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)



2 32% ↗ *2025: 10 (10%)*

Gorodenkoff / Shutterstock

Artificial intelligence

(e.g., implementation challenges, liability exposures, misinformation / disinformation)

3 29% ↘ *2025: 2 (31%)*

Aleksandr Medvedkov / Shutterstock

Business interruption

(incl. supply chain disruption)

4 26% → *2025: 4 (25%)*

Halkidkeriativemark / Adobe Stock

Changes in legislation and regulation

(e.g., tariffs, new directives, sustainability requirements)

5 21% ↘ *2025: 3 (29%)*

Bondarenkoth / Shutterstock

Natural catastrophes

(e.g., storm, flood, earthquake, wildfire)

6 19% ↘ *2025: 5 (19%)*

Bilanol / Shutterstock

Climate change

(e.g., physical, operational and financial risks as a result of extreme weather)

7 15% ↗ *2025: 9 (14%)*

Mr Nino / Shutterstock

Political risks and violence

(e.g., war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)

8 14% ↘ *2025: 7 (15%)*

fitpinkcat84 / Adobe Stock

Macroeconomic developments

(e.g., inflation, deflation, monetary policies, austerity programs)

9 13% ↘ *2025: 6 (17%)*

vichie81 / Shutterstock

Fire, explosion[1]

10 13% ↘ *2025: 8 (14%)*

Jo pix / Shutterstock

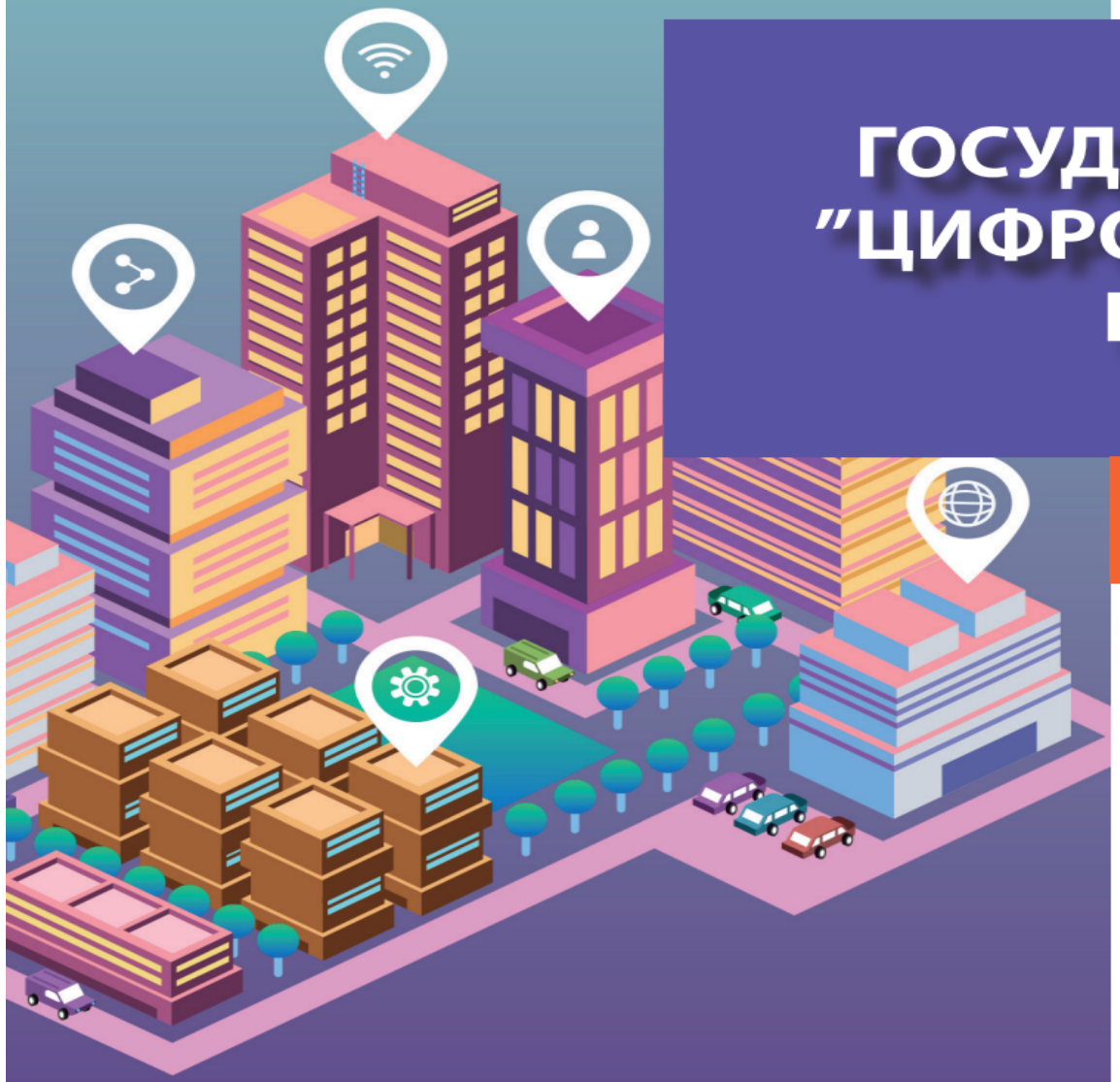
Market developments

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

Key

↑ Risk higher than in 2025
↓ Risk lower than in 2025
→ No change from 2025
(5%) 2025 risk ranking %

1 Fire, explosion ranks higher than market developments based on the actual number of responses
2 Critical infrastructure blackouts ranks higher than talent or labor issues based on the actual number of responses
3 Theft, fraud, corruption ranks higher than insolvency based on the actual number of responses
4 Loss of reputation or brand value ranks higher than biodiversity and nature risks based on the actual number of responses
5 Biodiversity and nature risks ranks higher than product recall, quality management, serial defects based on the actual number of responses



ГОСУДАРСТВЕННАЯ ПРОГРАММА ”ЦИФРОВОЕ РАЗВИТИЕ БЕЛАРУСИ“ НА 2021 – 2025 ГОДЫ

ЦЕЛЬ - внедрение информационно-коммуникационных и передовых производственных технологий в отрасли национальной экономики и сферы жизнедеятельности общества

4. Цифровое развитие отраслей экономики

5. Региональное цифровое развитие

3. Цифровое развитие государственного управления

6. Информационная безопасность и "цифровое доверие"

2. Инфраструктура цифрового развития

1. Информационно-аналитическое и организационно-техническое сопровождение цифрового развития

Государственная программа

состоит из 6 подпрограмм


КЛЮЧЕВЫЕ ЗАДАЧИ
Создание благоприятных условий для обеспечения процессов цифрового развития
Совершенствование национальной информационно-коммуникационной инфраструктуры и услуг
Совершенствование государственных функций (развитие технологий электронного правительства)
Повышение качества и доступности образования, основанного на применении современных ИТ
Повышение качества и доступности медицинского обслуживания населения на базе современных технических решений
Развитие инструментов цифровой экономики
Повышение уровня комфорта и безопасности жизнедеятельности населения (создание и внедрение технологий ”умных городов“)
Совершенствование системы информационной безопасности (формирование ”цифрового доверия“)

Мероприятия:

Создание национальной платформы контроля и реагирования на инциденты безопасности в ведомственных ИТ-инфраструктурах

Создание инфраструктуры мобильной и иных способов идентификации на базе Единой системы идентификации физических и юридических лиц

Создание системы сбора, обработки и анализа больших массивов неструктурированных данных специального назначения

Создание инфраструктуры облачной электронной цифровой подписи и доверенных сервисов на базе Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь

6. Подпрограмма ”Информационная безопасность и ”цифровое доверие“

Национальный центр кибербезопасности

В стране аттестовано

34

центра кибербезопасности

Руководитель несет персональную ответственность за обеспечение кибербезопасности

АКТУАЛЬНОСТЬ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

InDev Solutions

ОТВЕТСТВЕННОСТЬ РУКОВОДИТЕЛЯ

Указ президента Республики Беларусь 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации» в главе 3, п. 15 «Руководитель организации несет персональную ответственность за организацию работ по технический и криптографической защите информации в организации».

ТРЕБОВАНИЯ ПО КИБЕРБЕЗОПАСНОСТИ

- наличие актуальных схем;
- определение порядка генерации и смены паролей, обновления ПО;
- изменение установленных по умолчанию реквизитов доступа;
- использование модели разграничения доступа;
- идентификация и аутентификация пользователей, своевременное блокирование (удаление) неиспользуемых учетных записей;
- регламентированный доступ к администрированию;
- синхронизация системного времени от единого (общего) источника;
- межсетевое экранирование при внешнем взаимодействии;
- обнаружение и предотвращение вторжений при внешнем взаимодействии;
- защита от воздействия вредоносных программ;
- централизованный сбор и хранение событий безопасности (не менее года).

ЦИФРОВАЯ БЕЛАРУСЬ 2026-2030

InDev Solutions

Постановление Совета Министров Республики Беларусь от 30 декабря 2025 г. № 793

Экономика данных

- Новые стандарты связи
- Повышение качества данных государственных информационных ресурсов
- Внедрение прикладных цифровых решений

Цифровое государство

- Расширение электронных административных процедур
- Достижение «нулевой бюрократии»

Цифровой суверенитет

- Импортонезависимая экосистема программного обеспечения

Цель: формирование отечественной экосистемы цифровых решений для населения, бизнеса и государства, основанных на современной системе и инфраструктуре управления данными

КОНЦЕПЦИЯ РАЗВИТИЯ СИСТЕМЫ ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ ДО 2030 ГОДА

ГОИРО

- Цифровая трансформация процессов в системе образования
- Модернизация инфраструктуры системы образования
- Внедрение цифровых платформ дистанционного обучения при получении образования

КОНЦЕПЦИЯ РАЗВИТИЯ СИСТЕМЫ ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ до 2030

- ✓ внедрение средств автоматизации управления образовательным процессом в учреждениях образования;
- ✓ разработка электронных –образовательных ресурсов и технологий;
- ✓ разработка и ввод в эксплуатацию РИОС

- ✓ цифровизация процессов взаимодействия с предприятиями и государственными органами;
- ✓ разработка и внедрение автоматизированных систем управления учреждениями образования, интегрированных с республиканскими информационными системами (РИОС, ЕИОР) и сайтами УО;
- ✓ внедрение персонального цифрового профиля обучающегося;
- ✓ разработка информационно-аналитического портала качества образования (ИСУО)

КОНЦЕПЦИЯ РАЗВИТИЯ РИОС

Информационное ядро РИОС (ИЯ РИОС)	Регистр организаций	Регистр работников	Регистр обучающихся
Информационное ядро РИОС	Единая система аутентификации пользователей ИЯ РИОС	Единая система ведения справочников и классификаторов	Единая система администрирования и управления правами доступа
Образовательные платформы, сервисы и ресурсы	Централизованные облачные АСУ	Образовательные платформы, сервисы и ресурсы	Информационная система управления

Терминология в сфере информационной безопасности

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.
Иными словами – это практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации

Информационная инфраструктура – совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз (потенциально возможного ущерба)

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации

Терминология в сфере информационной безопасности

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры…в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации

Киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности

Распространение информации – действия, направленные на ознакомление с информацией неопределенного круга лиц

Предоставление информации – действия, направленные на ознакомление с информацией определенного круга лиц

Терминология в сфере информационной безопасности

Информационная система - совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств

Информационный ресурс - организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах

Комплекс программно-технических средств - совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий

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

Что и кого защищаем?

Объекты информационной инфраструктуры (среды) учреждения образования – средства вычислительной техники (СВТ, технические средства), сетевое оборудование, системное и прикладное программное обеспечение, информационные ресурсы и системы учреждения образования

Субъекты информационной среды учреждения образования (**пользователи**) – педагогические работники, иные работники учреждения образования, обучающиеся и их законные представители

Интернет-угрозы для инфраструктуры

Вывод компьютерной системы из строя, нарушение ее роботоспо-собности

Взлом (неправо-мерное вмешатель-ство в работу компьютерной системы)

Уничтожение или искажение информации

Раскрытие конфиден-циальной информации

Превышение полномочий непривиле-гированных пользователей

Интернет-угрозы для личности

Контентные риски	Коммуникационные риски	Электронные (технические риски)	Потребительские риски
• Вредоносная информация • Противозаконный контент • Неэтичная информация • Фейки	• Грумминг • Кибербуллинг • Троллинг • Буллицид	• Вредоносные программы • Кибермошенничество (фишинг, вишинг) • Спам	• Риски онлайн-маркетинга • Риски чрезмерных трат • Риск стать жертвой мошенника • Интернет-зависимость

Риски, связанные с обработкой персональных данных

- Утечка персональных данных
- Иски
- Жалобы в уполномоченный орган по защите персональных данных
- Отрицательные результаты проверок уполномоченного органа
- Приостановление (прекращение) обработки персональных данных в информационном ресурсе (системе)
- Привлечение к ответственности за нарушение порядка обработки ПнД

2025 г. (в процентах)

46 проверок деятельности операторов (плановые, внеплановые и камеральные проверки).

556 требований об устранении выявленных недостатков при обработке операторами (уполномоченными лицами) персональных данных (в 2024 году – порядка 370):

- по результатам рассмотрения поступивших жалоб субъектов персональных данных, обращений граждан и юридических лиц (297);
- по итогам мониторинга сети Интернет на предмет наличия документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных, обработки cookie-файлов операторами, осуществляющими продажу автомобилей, риэлтерскими организациями, организациями по государственной регистрации и земельному кадастру и т.п. (259).

Меры по защите персональных данных

1. Назначение ответственного за осуществление внутреннего контроля за обработкой персональных данных
2. Разработка положений об обработке персональных данных, о куки-файлах, перечня ИС с ПнД
3. Ознакомление работников, занятых обработкой ПнД, с документами и их обучение
4. Установление порядка доступа к ПнД
5. Обеспечение технической и криптографической защиты ПнД

Рекомендуемое содержание документов по обработке персональных данных оператора

Портфель оператора

Главная › Правовая основа › Портфель оператора

Портфель оператора

В рамках разъяснительной работы по вопросам применения законодательства о персональных данных в этом разделе размещаются примерн документов, которые следует принять оператору в целях реализации положений Закона о защите персональных данных.

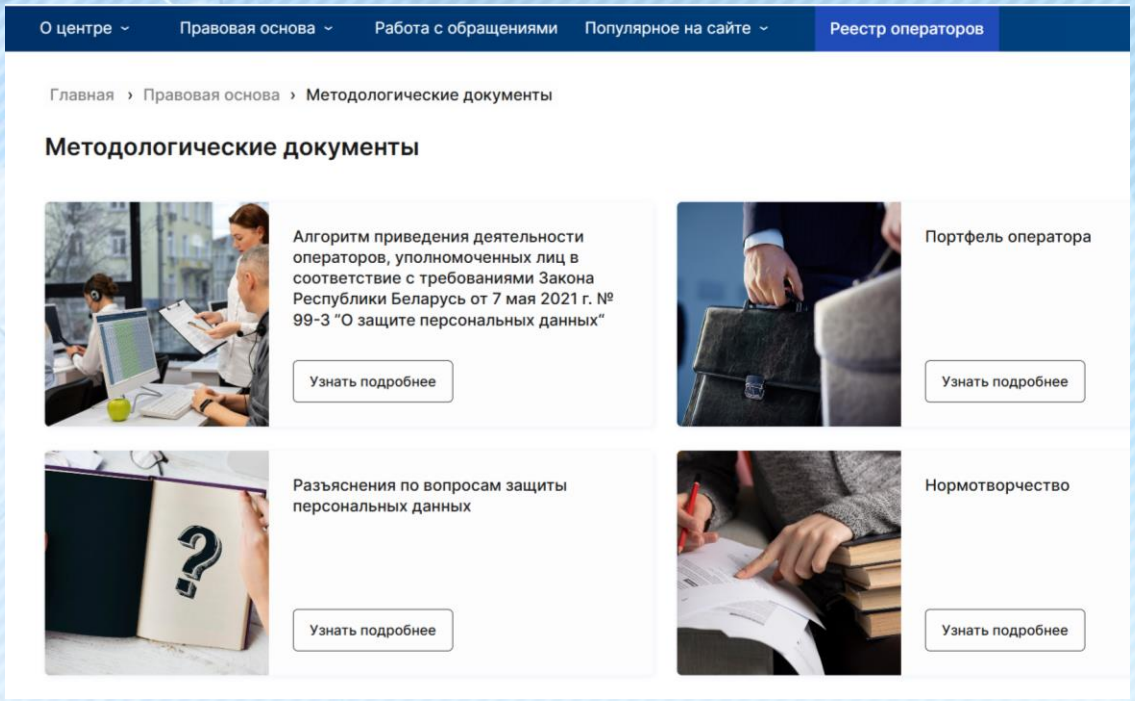
При адаптации формы к своему виду деятельности рекомендуем обращаться к рекомендациям и разъяснениям Центра, расположенным в ра «Методологические документы».

Политика в отношении обработки персональных данных в процессе трудовой деятельности и при осуществлении административных процедур

Организация уделяет особое внимание защите персональных данных при их обработке в нашей организации и с уважением относится к соблюдению прав субъектов персональных данных.
Утверждение Положения о политике в отношении обработки персональных данных в процессе трудовой деятельности и при осуществлен административных процедур (далее – Политика) является одной из принимаемых Организацией мер по защите персональных данных...

Реестр обработки персональных данных (примеры)

Перечень уполномоченных лиц, обрабатывающих персональные данные: ООО "Белорусские облачные технологии", Национальный центр р информации Республики Беларусь, РУП "Национальный центр электронных услуг"...



Меры по защите информации

1. Правовые

2. Технические

3. Организационные

Ключевые нормативные правовые акты в сфере защиты информации

Постановление Совета безопасности Республики Беларусь 18 марта 2019г. №1 «О Концепции информационной безопасности Республики Беларусь»

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

Приказ ОАЦ от 20 февраля 2020 года №66

Закон Республики Беларусь от 19 ноября 1993 года №2570-XII «О правах ребенка»

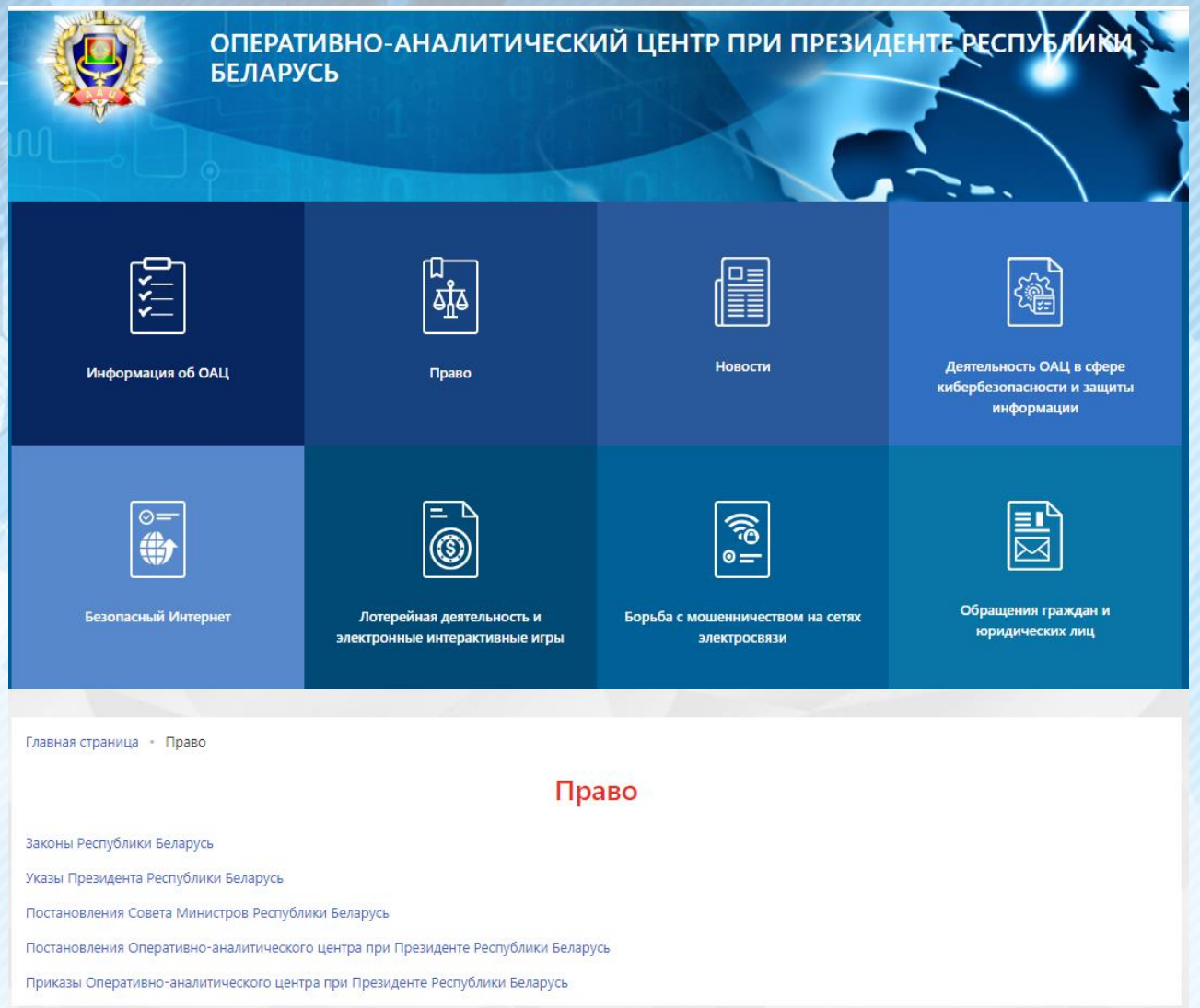
Закон Республики Беларусь от 10 ноября 2008 года №455-З «Об информации, информатизации и защите информации»

Указ Президента Республики Беларусь 14 февраля 2023 года №40 «О кибербезопасности»

Закон Республики Беларусь от 17 июля 2008 года №427-З «О средствах массовой информации»

Актуальные НПА на сайте ОАЦ

https://www.oac.gov.by/law

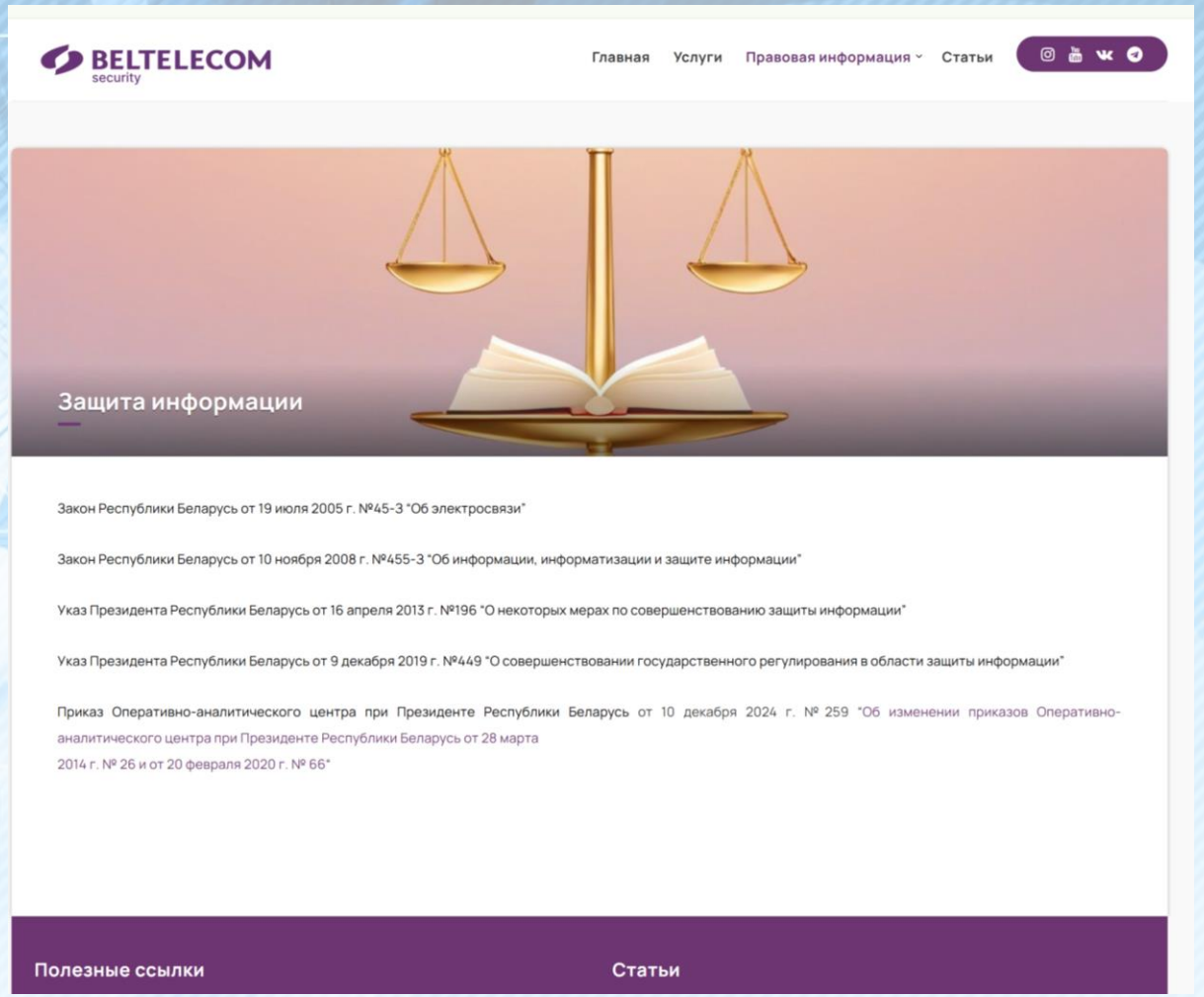


Актуальные НПА на сайте Министерства связи и информатизации

https://www.mpt.gov.by/ru/kiberbezopasnost

Актуальные НПА на сайте РУП «Белтелком»

https://security.beltelecom.by/



УТВЕРЖДАЮ

Заместитель Премьер-министра
Республики Беларусь

В.М.Каранкевич

№ 33/202-390/

КОМПЛЕКСНЫЙ ПЛАН

мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2026 – 2027 годы

Современное общество живет в эпоху беспрецедентного распространения технологий, при котором цифровизация становится одной из основных движущих сил развития различных сфер человеческой деятельности. Наряду с совершенствованием технологических процессов получают развитие электронные сервисы: финансовые услуги, дистанционное управление устройствами, удаленная работа и учеба, интернет-торговля, социальные и нейросети. Они прочно вошли в повседневную жизнь, упрощая быт, повышая комфорт, улучшая качество жизни граждан.

Государственное управление, промышленность, финансовая система, образование, здравоохранение, инфраструктура, услуги – все эти фундаментальные аспекты современности используют цифровые технологии.

Наряду с безграничными возможностями всеобщая цифровизация несет новые вызовы и угрозы. Глобальная компьютерная сеть Интернет, созданная как платформа для свободного обмена информацией и сотрудничества, все чаще становится полем для преступной деятельности. Киберпреступность представляет собой одну из наиболее серьезных опасностей современности, являясь организованной, высокотехнологичной и финансово мотивированной системой, способной наносить колоссальный ущерб.

УТВЕРЖДАЮ
Председатель Гомельского областного исполнительного комитета
И.И.Крупко
«4» марта 2026 года

ОБЛАСТНОЙ КОМПЛЕКСНЫЙ ПЛАН
мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2026 – 2027 годы

Современный мир характеризуется динамичными глобальными процессами. Совершенствование информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие, она превращается в системообразующий фактор жизни людей, общества и государства. Усиливается роль и влияние средств массовой информации, глобальных коммуникационных механизмов на экономическую, политическую и социальную ситуацию. Информационные технологии находят широкое применение в управлении важнейшими объектами жизнеобеспечения, которые становятся более уязвимыми перед случайными и преднамеренными воздействиями.

В этих условиях киберпреступность представляет собой одну из наиболее актуальных и динамично развивающихся угроз в современном мире, и Республика Беларусь не является исключением.

Значительное число киберпреступлений обусловлено рядом причин: интенсивность процесса развития системы безналичных расчетов, увеличение пользователей электронных платежных систем и держателей банковских платежных карт, интернет-пользователей, абонентов сотовой связи.

Также одной из основных причин роста преступлений в киберсфере является недостаточная цифровая грамотность граждан в сфере защиты персональных данных.

Перечень первоочередных мер для создания системы защиты информации

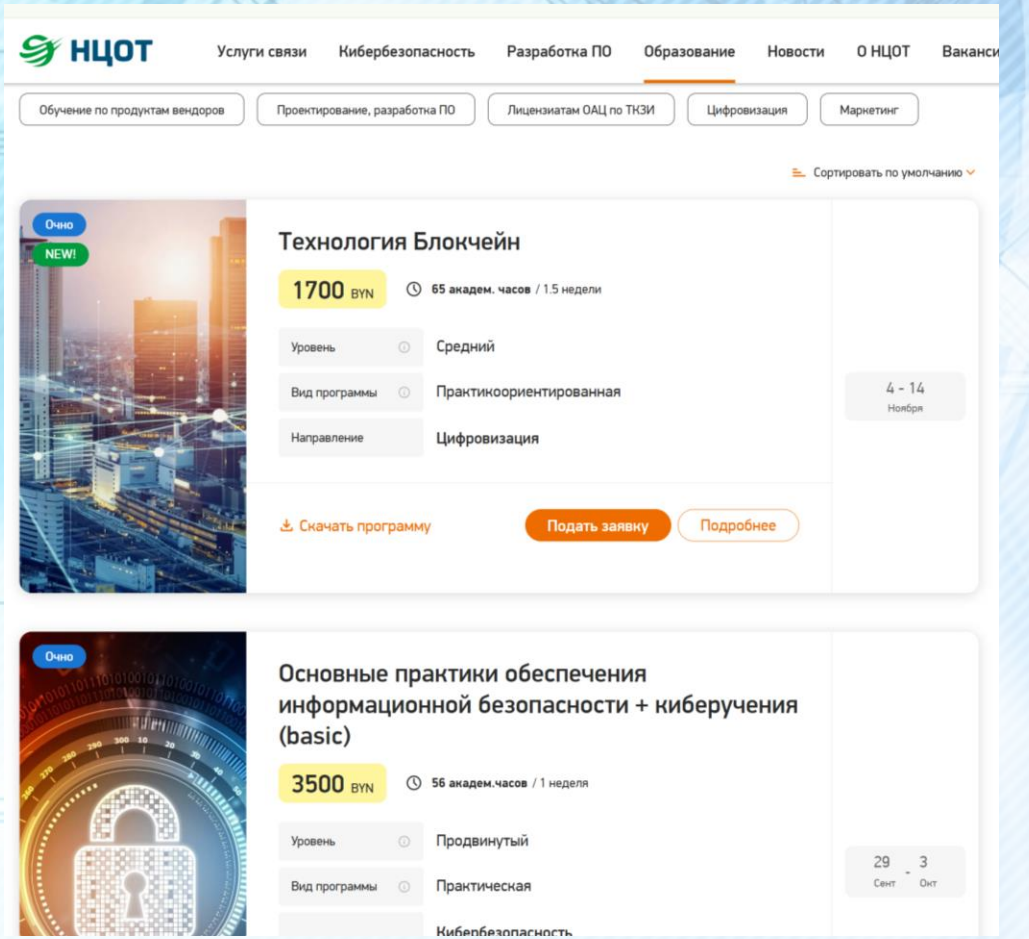
1. Направлен ОАЦ в начале 2022 года для реализации в целях обеспечения кибербезопасности информационных сетей, систем и ресурсов

2. Касается всех УО. Состоит из 3 частей в составе 40 пунктов на шести страницах

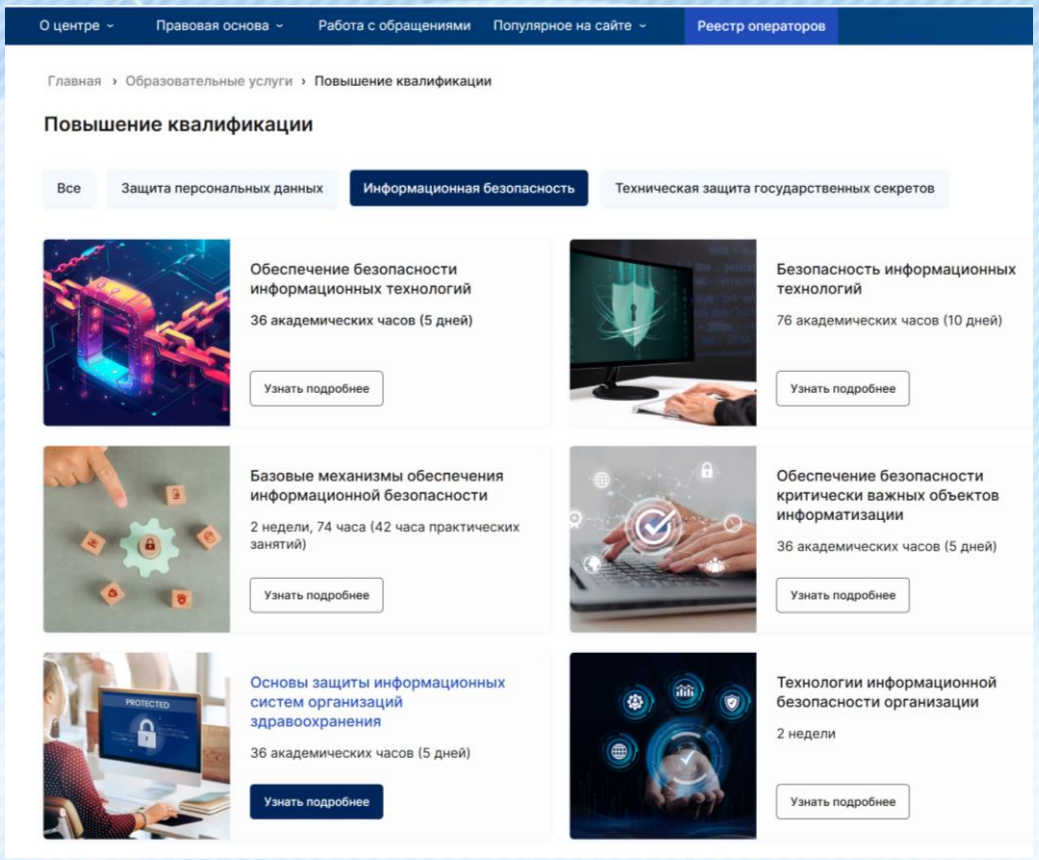
3. Требует обеспечить прохождение переподготовки или повышение квалификации, работников ответственных за защиту информации

Повышение квалификации лиц, ответственных за информационную безопасность

https://ncot.by/ru/obrazovanie/povyshenie2/



https://cpd.by/obrazovatelnie-uslugy/o-povyshenii-kvalifikatsii-v-tsentre/



Система защиты информации в информационных сетях

Меры разработаны в соответствии с законодательством Республики Беларусь и направлены на исключение условий для компрометации информационных сетей и систем государственных органов и организаций, а также повышение их защищенности.

Владельцам (собственникам) информационных систем необходимо **выполнить ряд мероприятий в установленные сроки: месячный, трехмесячный и шестимесячный.**
Также определены меры, которые следует регулярно осуществлять в процессе эксплуатации информационных ресурсов и систем.

Первоочередные меры (месячный срок)

Категорирование информации

Осуществить категорирование информации, обрабатываемой в информационных сетях (системах).

Анализ структуры сетей

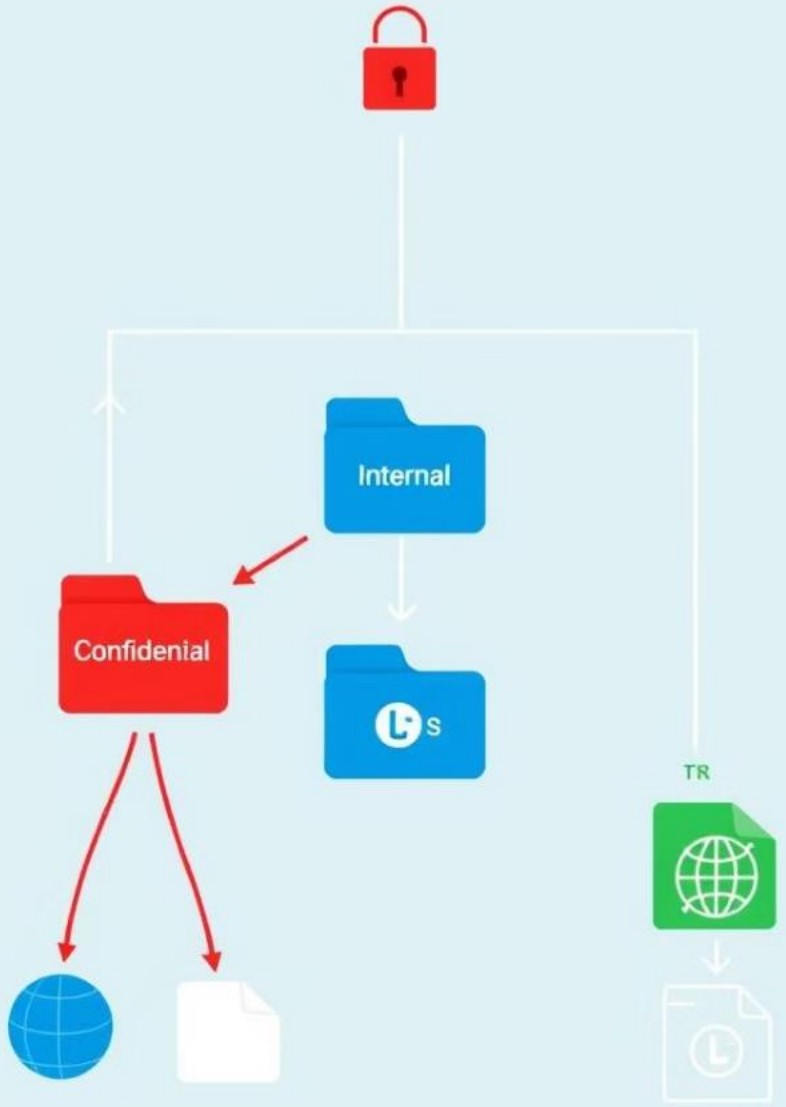
Провести анализ структуры информационных сетей и информационных потоков в целях определения состава и мест размещения объектов, их физических и логических границ.

Внедрение средств защиты

Осуществить выбор и внедрение средств технической защиты информации с учетом рекомендаций изготовителя и ограничений, указанных в сертификатах соответствия.

Смена реквизитов доступа

Осуществить смену реквизитов доступа к функциям управления и настройкам, установленным по умолчанию.



Управление программным обеспечением (месячный срок)

Разрешенное ПО

Определить перечень разрешенного программного обеспечения и регламентировать порядок его установки и использования.

Учетные записи

Обеспечить использование объектов информационной сети под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов или их особенностей функционирования).

Обновления

Обеспечить обновление программного обеспечения объектов информационной сети из доверенных источников и контроль за своевременностью такого обновления.

Защита от вредоносных программ

Обеспечить защиту средств вычислительной техники от вредоносных программ.

Сетевая безопасность (месячный срок)

Сегментирование сети

Обеспечить сегментирование (изоляцию) сети управления объектами информационной сети от сети передачи данных.

Управление информационными потоками

Обеспечить управление внешними информационными потоками (маршрутизация) между информационными сетями.
Использовать маршрутизатор либо коммутатор маршрутизирующий.

Фильтрация трафика

Обеспечить ограничение входящего и исходящего трафика (фильтрация) информационной сети только необходимыми соединениями. Использовать межсетевые экраны, функционирующие на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях.

Контроль внешних подключений

Обеспечить контроль за внешними подключениями к информационным сетям.

Документация по безопасности (трехмесячный срок)

Политика информационной безопасности

Разработать либо скорректировать политику информационной безопасности, определяющую цели и принципы защиты информации, перечень информационных систем, сведения о подразделениях защиты информации, обязанности пользователей и порядок взаимодействия с иными системами.

Общая схема системы защиты

Осуществить разработку общей схемы системы защиты информации, включающей наименование системы, класс, места размещения объектов, физические границы, внешние и внутренние информационные потоки.

Техническое задание

Разработать либо скорректировать техническое задание на информационные системы, определяющее наименования систем, требования к системе защиты информации, сведения о взаимодействии с иными системами, порядок обезличивания персональных данных и требования к средствам криптографической защиты.

Документация на систему защиты

Разработать документацию на систему защиты информации в соответствии с техническим заданием, описывающую порядок разграничения доступа, резервирования, защиты от вредоносного ПО и другие аспекты безопасности.

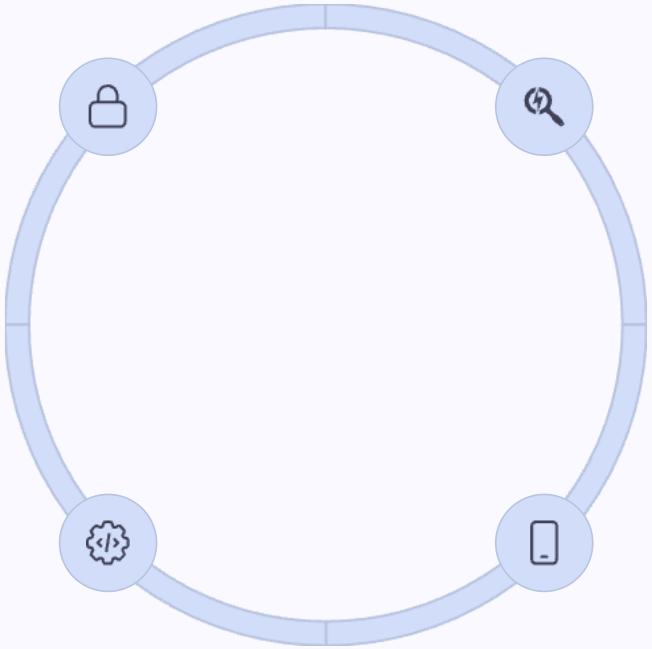
Криптографическая защита и мониторинг (трехмесячный срок)

Криптографическая защита

Осуществить выбор и внедрение средств криптографической защиты информации с учетом рекомендаций изготовителя и ограничений, указанных в сертификатах соответствия.

Контроль функционирования

Обеспечить контроль за работоспособностью, параметрами настройки и правильностью функционирования объектов информационной сети.



Мониторинг событий

Определить способ и периодичность мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационных сетей.

Мобильные устройства

Регламентировать порядок использования в информационной сети мобильных технических средств и контроля за таким использованием.

Положении о порядке аттестации систем защиты информации

Наличие аттестата соответствия является обязательным условием для обработки информации, распространение и (или) предоставление которой ограничено

Аттестация проводится организациями, имеющими специальные разрешения (лицензии) на деятельность по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ (далее – специализированные организации).
Собственники (владельцы) информационных систем вправе самостоятельно проводить аттестацию

Аттестат соответствия оформляется сроком на пять лет

Положение о порядке технической и криптографической защиты информации

Обязательно для владельцев (собственников) информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам

Определяет порядок создания и функционирования системы защиты информации

Определяет тех, кто выполняет работы по тех. и криптограф. защите информации у собственника (владельца)

Классы типовых информационных систем

1. Класс 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.
2. Класс 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.

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

ПРИКАЗ ОАЦ ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
12 ноября 2021 г. № 195

Классы типовых информационных систем

5. Класс 4-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных.
6. Класс 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.
7. Класс 4-бг – информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных.
8. Класс 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.
9. Класс 4-дсп – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных.

Классы типовых информационных систем

10. Класс 3-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.
11. Класс 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.
12. Класс 3-бг – информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных.
13. Класс 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.
14. Класс 3-дсп – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных.

ИМП Министерства образования Республики Беларусь от 18.08.2025 г.

ГОИРО

УТВЕРЖДАЮ
Заместитель Министра образования
Республики Беларусь
_____ В.В.Долженков
_____ 2025 г.

ИНСТРУКТИВНО-МЕТОДИЧЕСКОЕ ПИСЬМО МИНИСТЕРСТВА ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
«Об использовании современных информационно-коммуникационных технологий в учреждениях общего среднего образования в 2025/2026 учебном году»

1. Общие положения

Инструктивно-методическое письмо Министерства образования Республики Беларусь «Об использовании современных информационно-коммуникационных технологий в учреждениях общего среднего образования в 2025/2026 учебном году» (далее – ИМП) содержит рекомендации для учреждений общего среднего образования при использовании современных информационно-коммуникационных технологий (далее – ИКТ) в образовательном процессе.

Цели цифровой трансформации процессов в системе образования:

способствовать подготовке обучающихся к жизни в цифровом обществе;

подготовить систему образования к работе в условиях быстрых изменений – к внедрению инновационных технологий, изменению образовательных парадигм, гибкому формированию требований и программ;

способствовать оптимизации процессов, протекающих в системе образования;

1.6. Информационная безопасность в учреждениях среднего образования

2.6.1. Цель информационной безопасности

Целью обеспечения безопасности информации является обе конфиденциальности, целостности, подлинности, дос и сохранности информации, которая используется в учреждения среднего образования.

В соответствии с Законом Республики Беларусь «Об инф информатизации и защите информации» в зависимости от доступа информация делится на общедоступную инф и информацию, распространение и (или) предоставление ограничено.

Защите подлежит информация, неправомерные действия в от которой могут причинить вред ее обладателю, пользователю и лицу.

Требования по защите общедоступной информации устанавливаться только в целях недопущения ее унич модификации (изменения), блокирования правомерного доступа

Информация, распространение и (или) предоставление ограничено, не отнесенная к государственным должна обрабатываться в информационных системах с прим системы защиты информации, аттестованной в порядке, устан Оперативно-аналитическим центром при Президенте Ре Беларусь.

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

Обеспечение целостности и сохранности информации, содер в информационной системе, осуществляется путем уста и соблюдения единых требований по защите инф от неправомерного доступа, уничтожения, модификации (из и блокирования правомерного доступа к ней, в том при осуществлении доступа к информационным сетям.

2.6.2. Задачи информационной безопасности

Основными задачами учреждений образования в части обе безопасности информации являются:

обеспечение эффективного, надежного и бе функционирования информационных систем и ресурсов, которые используются в учреждениях образования;

предупреждение (предотвращение) нарушений информационной безопасности;

своевременное обнаружение нарушений информационной

безопасности;

выполнение требований действующего законодательства в области информации, информатизации и защиты информации, а также других нормативных правовых актов в части информационной безопасности.

2.6.3. Объекты защиты системы информационной безопасности

Основными объектами защиты являются:

информационные ресурсы, содержащие распространение и (или) предоставление которой огра открыто распространяемая информация, необходима независимо от формы и вида ее представления;

информационная инфраструктура, включающая си и анализа информации, технические и программные средс передачи и отображения, в том числе каналы информа и телекоммуникации, системы и средства защиты инфо и помещения, в которых размещены такие информац и ресурсы.

2.6.4. Угрозы информационной безопасности

Угрозы информационной безопасности – это разл которые могут привести к нарушениям информационн Другими словами, это потенциально возможные с или действия, которые могут нанести ущерб и и компьютерным системам.

Угрозы могут быть реализованы только при налич уязвимостей, присущих объекту информатизации.

В качестве источников угроз могут выступать (физические лица), так и объективные причины появлени отметить, что источники угроз могут находиться как вну организации (учреждения) – внутренние источники, так и источники.

В зависимости от различных способов классификаци угрозы информационной безопасности можно разделит основные подгруппы:

нежелательный контент;

несанкционированный доступ;

утечки информации;

потеря данных;

мошенничество;

кража информации;

халатность сотрудников;

вредоносные программы;

аппаратные и программные сбои;

хакерские атаки;

спам.

2.7. Рекомендации по обеспечению информационной безопасности

2.7.1. Парольная защита

Для обеспечения безопасности пароля рекомендуется:

составлять пароль не менее чем из 8 символов, которые включают в себя буквы разного регистра, цифры и специальные символы;

сохранять в тайне личный пароль, никогда не сообщать пароль другим лицам и не хранить записанный пароль в общедоступных местах;

в случае производственной необходимости (командировка, отпуск и т.п.) при проведении проверочных мероприятий, допускается раскрытие значений своего пароля руководителям подразделений. По окончании производственных или проверочных работ работники самостоятельно производят немедленную смену значений «раскрытых» паролей;

не использовать пароль доступа в локальную сеть организации в других программах и на сайтах, где требуется регистрация;

не сохранять пароли в программах, большинство программ хранят их в открытом виде и тот, кто получит доступ к компьютеру, получит доступ и к ним.

2.7.2. Антивирусная защита

Антивирусное программное обеспечение, установленное на компьютере, не следует отключать.

Необходимо обязательно проверять на наличие вирусов все внешние носители информации (диски, флешки, внешние твердотельные накопители, внешние жесткие диски и т.п.), поступающие со стороны (из внешних организаций, других подразделений организации и т.п.).

Во всех случаях возможного проявления действия вирусов или при подозрении на наличие вирусов не следует пытаться удалить вирусы самостоятельно, необходимо незамедлительно сообщить об этом ответственному за антивирусный контроль и оценить с ним возможные пути заражения и распространения вируса.

Необходимо периодически проводить проверку жесткого диска и/или твердотельного накопителя антивирусным программным обеспечением.

2.7.3. Интернет и электронная почта

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, следует обязательно проверять на отсутствие вредоносных программ и вирусов.

Не следует:

Организационно-правовые меры по защите информации: издание приказов

Назначение ответственных лиц (за меры по защите информации, внутренний контроль за обработкой персональных данных, за сайт и электронную почту)

Утверждение регламентов по работе с официальными интернет-сайтом и почтой, а также политик информационной безопасности и обработки персональных данных и других связанных документов

Примерная структура «Регламент электронной почты учреждения образования»

1.Общие положения,
где прописывается назначение регламента, наименование адреса(ов) электронной почты

2. Функции ответственных,
где прописывается кто отвечает за организацию предоставления писем и передачу их ответственным за рассылку и т.д.

3. Технические требования к электронным письмам

ИМП Министерства образования Республики Беларусь «Об использовании современных информационных технологий в учреждениях общего среднего образования в 2025/2026 учебном году»

1.4. Корпоративная электронная почта

Для работы с системой обмена электронными сообщениями (электронной почтой) в учреждениях образования необходимо использовать серверы электронной почты провайдеров, которые располагаются на территории Республики Беларусь. Со списком уполномоченных поставщиков интернет-услуг можно ознакомиться на сайте Оперативно-аналитического центра при Президенте Республики Беларусь (https://oac.gov.by/Internet-service-providers/secure-internet/information-internet-service-providers-hosting). Использование бесплатных почтовых сервисов (gmail, яндекс.почта, mail.ru и т.п.) в рабочих целях является недопустимым.

Интернет-услуги, в том числе сервера электронной почты провайдеров, для использования учреждениями образования в рабочих целях регламентируются Указом Президента Республики Беларусь от 18.09.2019 № 350 «Об особенностях использования национального сегмента сети Интернет».

Примерная структура «Регламент о работе официального интернет-сайта учреждения образования»

1.Общие положения,
где прописывается место размещения сайта и его назначения

2. Функции ответственных
за предоставление, размещение информации, техническое сопровождение

3. Порядок предоставление,
размещения информации, техническое требования к ней

Приложение.
Порядок заполнения разделов официального интернет-сайта

№ пп	Раздел (рубрика)	Ответственный за предоставление информации	Периодичность обновления информации
1	Новости	Проректоры, руководители структурных подразделений	Ежедневно

Обязательные мероприятия плана

Спланировать закупки оборудования и услуг

Разработать порядок или регламенты по работе с официальными интернет-сайтом и почтой

Создать комиссию по отнесению информационной системы к классу типовых информационных систем, оформить акты отнесения информационной системы к классу типовых ИС

Разработать положение о политике информационной безопасности и положение о политике обработки персональных данных и др. сопутствующие локальные документы

Ознакомить работников с документами по защите информации и обработке персональных данных (под роспись), обучить ответственных и других работников

Политика информационной безопасности

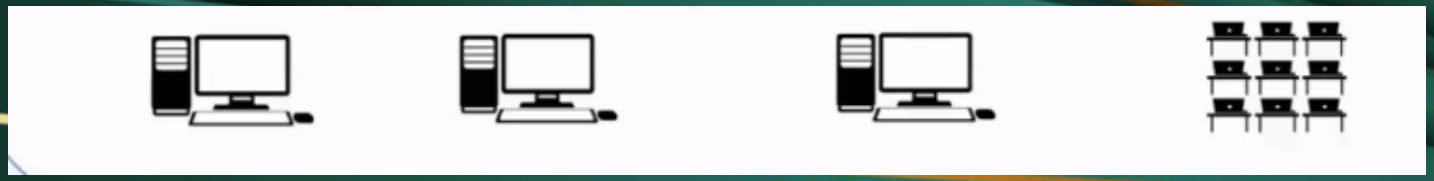
- общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, документально закрепленные собственником (владельцем) информационной системы

Должна содержать:

- цели и принципы защиты информации;
- перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем, перечень средств вычислительной техники, а также сведения о подразделениях защиты информации или ином подразделении (должностном лице), ответственном за обеспечение защиты информации *(+ перечень разрешенного ПО);*
- обязанности пользователей информационных систем;
- порядок взаимодействия с иными информационными системами;
- *+ другое*

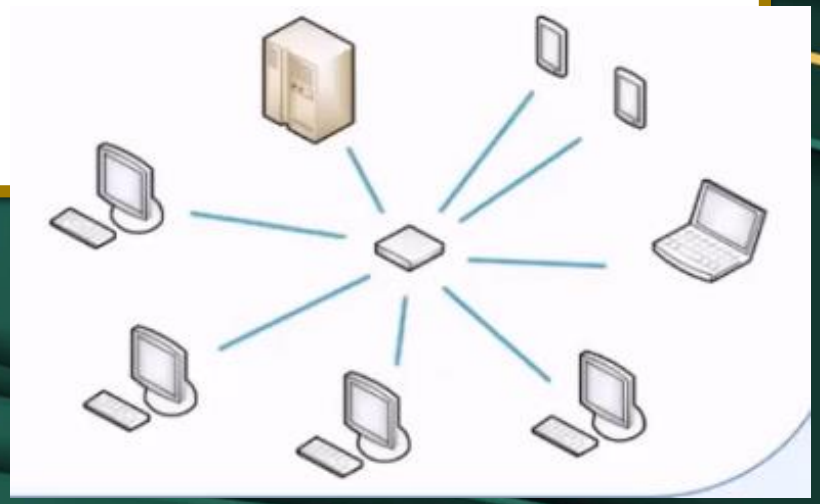
Обеспечение защиты СВТ: простая инфраструктура

1. Настройка парольного доступа (например, учетные записи администратор, работник, учащийся)
2. Установка антивирусного программного обеспечения
3. Отключение функции автозагрузки внешних машинных носителей (флешки и т.п.)
4. Обучать цифровой гигиене при пользовании Интернетом и электронной почтой
5. Проверить в договорах с Белтелекомом наличие услуги фильтрации трафика (профиль №7 или «Родительский контроль»)
6. Контроль доступа в помещении с объектами информационной среды
7. Программное обеспечение устанавливают и своевременно обновляют только администраторы



Обеспечение защиты СВТ: сложная инфраструктура

1. Настройка контроллера домена для централизованного управления пользователями и разграничения прав доступа
2. Настройка брэндмауэра (межсетевого экрана) на серверах
3. Проксирование сетевого трафика (установка прокси-сервера)
4. Установка антивирусного программного обеспечения на серверах
5. Синхронизация системного времени от единого источника
6. Резервирование информации
7. Удаленный доступ – VPN-канал (Белтеком или на своих ресурсах)



Информация Министерства внутренних дел Республики Беларусь по профилактике киберпреступлений (аудио-, видеоролики, инфографика, памятки)

Республиканский список экстремистских материалов размещен на сайте Министерства информации Республики Беларусь mininform.gov.by

Чек-лист для педагогов

- ✔ Используйте последние обновления
- ✔ Не устанавливайте самостоятельно
- ✔ Используйте двухэтапную аутентификацию
- ✔ Используйте надежные пароли
- ✔ Переходите по ссылкам осторожно
- ✔ Оповестите остальных об атаке
- ✔ Всегда помните о мошенниках (*рекомендации ОАЦ*)
- ✔ Старайтесь не сообщать личную информацию в социальных сетях
- ✔ Защитите физические устройства

Направления работы с родителями

- Знакомство с интернет-угрозами и способами защиты
- Обучение выявлению и способам защиты ребенка от кибербуллинга
- Обучение помощи жертвам кибернасилия
- Профилактика интернет-зависимости у ребенка (*ПО родительского контроля*)
- Обучение безопасному и ответственному поведению в сети

Направления работы с обучающимися

- Обучение правилам ответственного поведения в сети
- Знакомство с интернет-угрозами и способами защиты
- Профилактика и (по возможности) пресечение всех видов сетевой агрессии
- Обучение выявлению и способом защиты от кибербуллинга и киберхарассмента
- Помощь жертвам кибернасилия
- Профилактика интернет-зависимости

РЕКОМЕНДАЦИИ РОДИТЕЛЯМ:

- храните имена пользователей и пароли в безопасности;
- периодически меняйте пароли;
- не разглашайте личную информацию о себе и детях в Интернете, которая могла бы помочь интернет-хищникам найти ваших детей;
- будьте внимательны в социальных сетях. Напомните детям, что все опубликованное в Интернете сразу становится общедоступным;
- объясните опасность передачи геоданных;
- создайте совместно с детьми список правил использования Интернета;

- используйте одинаковые правила при общении онлайн и лично;
- научите детей тому, что к онлайн и к личному общению применимы одни и те же правила;
- установите родительский контроль;
- используйте антивирусные программы на всех устройствах;
- расскажите о существовании фальшивых рекламных объявлений;
- объясните детям об опасности личных встреч с незнакомцами;
- периодически смотрите истории поиска в Интернете

Продемонстрируйте детям максимальную открытость при отслеживании их действий в Интернете, чтобы они не ощущали, что за ними шпионят.

ОРГАНИЗАЦИЯ РАБОТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ В УЧРЕЖДЕНИИ ОБРАЗОВАНИЯ

КАЦУБА В.Ю.,
начальник учебно-методического отдела
информационных технологий и издательской деятельности
it@iro.gomel.by