УТВЕРЖДАЮ
Генеральный директор
СЗАО «Интерднестрком»
Ганжа С.Н.
«___»_____ 2021г.

ИНСТРУКЦИЯ
по организации антивирусной защиты в СЗАО «Интерднестрком»

1. Общие положения

1.1. Настоящая Инструкция является обязательной для исполнения всеми сотрудниками Компании, эксплуатирующими средства вычислительной техники.

1.2. Антивирусная защита - комплекс правовых, организационных, технических и технологических мер, применяемых для обеспечения защиты средств вычислительной техники и информационных систем от воздействия компьютерных вирусов.

1.3. Компьютерные вирусы - это специально разработанные программы, программные модули, блоки, группы команд, умышленно включаемые в программное обеспечение с целью дезорганизации вычислительного процесса (существенного замедления обработки информации), осуществления модификации (изменения, стирания) хранящихся на магнитных носителях программ и данных.

1.4. Антивирусное средство - программное средство, предназначенное для выявления фактов вирусного воздействия на средства вычислительной техники и обладающее средствами восстановления их исходного состояния.

1.5.1. Целями антивирусной защиты является противодействие угрозам нарушения целостности обрабатываемой информации, сохранение работоспособности информационной системы и её восстановление с минимальными финансовыми издержками и временными затратами.

1.6. Основными принципами антивирусной защиты являются:

- использование в работе только лицензионного программного обеспечения;
- проверка всех съемных носителей информации и файлов, полученных по электронной почте, из Интернета или от организаций, на наличие вирусов перед их использованием;
- периодическая проверка средств вычислительной техники на наличие вирусов, с использованием последней версии антивирусной программы.

1.7. Инструкция регламентирует действия сотрудников подразделений Компании при организации антивирусной защиты электронных технологий предприятия.

2. Организация антивирусной защиты

2.1. Реализация мероприятий антивирусной защиты возложена на специалиста, ответственного по защите информации, и специалиста по информационному обеспечению.

2.2. На специалиста, ответственного по защите информации, возлагается:

- разработка и согласование проектов нормативных документов по организации антивирусной защиты;
- определение потребностей в антивирусных средствах;
- анализ состояния антивирусной защиты, разработка мероприятий по ее совершенствованию;
- внесение предложений по ежегодной закупке антивирусного программного обеспечения, продлению договоров на его техническую поддержку и сопровождение.

2.3. На специалиста по информационному обеспечению возлагается:

- регулярное получение новых версий антивирусного программного обеспечения, систематическое обновление антивирусных баз;
- доведение программного обеспечения до всех сотрудников структурных подразделений предприятия, эксплуатирующих средства вычислительной техники;
- контроль за осуществлением антивирусной защиты;
- проведение расследований случаев заражения средств вычислительной техники вирусами, принятие мер к локализации и уничтожению вирусов.

3. Установка и обновление антивирусных средств

3.1. К применению в Компании допускаются лицензионные антивирусные средства.

3.2. Установка и регулярное обновление антивирусных средств осуществляется специалистом по информационному обеспечению.

3.3. Антивирусные средства устанавливаются на соответствующих серверах Компании и рабочих станциях в структурных подразделениях Компании.

3.4. Обновление антивирусного программного обеспечения производится по мере получения новых версий. Антивирусные базы обновляются автоматически 1 раз в день.

4. Контроль над осуществлением антивирусной защиты

4.1. Установка (изменение) антивирусного программного обеспечения компьютера должна осуществляться только специалистом по информационному обеспечению или специалистом, ответственным по защите информации.

4.2. Настройка антивирусных средств должна обеспечивать автоматический контроль на наличие компьютерных вирусов при каждой перезагрузке компьютера (для серверов локально-вычислительной сети - при перезапуске).

4.3. Обязательной проверке на отсутствие компьютерных вирусов подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация со съёмных носителей (магнитные диски, CD-ROM, флеш-накопители и т.п.), получаемых от сторонних лиц и организаций.

4.4. Контроль информации на съёмных носителях производится перед её использованием непосредственно в структурных подразделениях Компании.

5. Действия при обнаружении компьютерного вируса

5.1. При возникновении подозрения на наличие компьютерного вируса сотрудник структурного подразделения Компании должен провести внеочередную проверку на наличие или отсутствие компьютерного вируса.

5.2. При обнаружении компьютерного вируса необходимо:

- приостановить работу, поставить в известность о факте обнаружения заражённых вирусом файлов руководителя структурного подразделения Компании, соответствующего специалиста СИТ, владельца этих файлов, а также структурные подразделения Компании, использующие эти файлы в работе;
- совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение заражённых вирусом файлов антивирусными средствами, при невозможности или неэффективности лечения уничтожить заражённые вирусом файлы способом, исключающим их восстановление.

6. Ответственность при организации антивирусной защиты

6.1. Руководители структурных подразделений Компании несут персональную ответственность за антивирусную защиту в своих структурных подразделениях,

осуществляя постоянный контроль над выполнением сотрудниками структурного подразделения правил антивирусной защиты информации.

6.2. Ответственность за выполнение положений настоящей Инструкции возлагается на руководителей структурных подразделений.

6.3. Периодический контроль над соблюдением положений настоящей Инструкции возлагается на специалиста, ответственного по защите информации.