Для обеспечения должного уровня информационной безопасности необходимо выполнять следующие требования.

Разработать (*в случае отсутствия данного ЛНПА на объекте*) либо переработать (*в случае отсутствия ниже приведенных требований*) и утвердить у руководства предприятия, организации политику информационной безопасности, включив в нее в обязательном порядке и обеспечив действенное выполнение следующих требований:

- возложение обязанностей по обеспечению контроля за ее соблюдением на конкретного специалиста (*должностное лицо*), обладающего соответствующими знаниями и опытом профессиональной деятельности;
- обязательное составление ответственными специалистами (*должностными лицами*) докладных записок (*иных документов*) на имя непосредственных руководителей по каждому установленному факту нарушения политики безопасности, проведение по ним служебных разбирательств с принятием необходимых мер реагирования;
- меры ответственности за факты нарушения политики безопасности как со стороны ответственных лиц, так и иных работников предприятия, организации;
- исключение возможности использования сторонних Машинных Носителей Информации –МНИ (*флешки, жесткие диски и т.д.*) на рабочих местах без предварительной проверки содержимого на предмет вредоносного ПО ответственными за соблюдение политики безопасности;
- разграничение доступа пользователей при работе на ПЭВМ (*создание персональных учётных записей с соблюдением требований политики безопасности паролей, своевременная смена реквизитов доступа пользователей к информации*), а также использование ограниченных пользовательский учетных записей, исключающих возможность установки дополнительного программного обеспечения;
- запрет на хранение паролей к учётным записям пользователей в текстовых или иных файлах на локальных дисках;
- своевременное и регулярное создание резервных копий файловой системы (*back-up*) с сохранением на отдельных серверах или в облачных хранилищах данных;
- протоколирование и документирование (*ведение log-файлов*) действий всех пользователей (использование штатных средств операционных систем и/или DLP-систем);
- ограничение удаленного доступа к средствам вычислительной техники; при необходимости использования удаленного доступа – осуществление настройки сетевого оборудования для удаленного доступа

исключительно выделенным кругом лиц с указанием конкретных IP или MAC-адресов рабочих станций;

- обязательное изменение заводских реквизитов доступа (*логин и пароль*) вновь приобретаемого и монтируемого сетевого оборудования;
- использование исключительно сертифицированных ОАЦ РБ лицензионных антивирусных программных продуктов на рабочих станциях и серверах;
- исключение доступа посторонних лиц, в том числе работников обслуживающих организаций, к служебной информации, хранящейся в информационных системах и СВТ, паролям доступа, а также обеспечение контроля за использованием указанными лицами внешних запоминающих устройств;
- обеспечение жесткого контроля за физическим доступом к местам размещения СВТ, обрабатывающих критически важную информацию;
- обеспечение физической изоляции контуров бухгалтерского и кадрового учета, а также иных информационных систем, содержащих служебную информацию, от общей сети организации и от сети Интернет, за исключением случаев наличия аттестованных в установленном порядке систем защиты информации таких информационных систем. Выгрузка информации на порталы ФСЗН, ИМНС и т.п. должна осуществляться с использованием флеш-накопителя на отдельном ПК, оснащенном антивирусным ПО и имеющим доступ в сеть Интернет только на необходимые ресурсы (порталы). Использование таких флеш-накопителей для иных целей не допускается.
- для обмена сведениями посредством Интернет-почты использование только **защищенных сервисов** электронной почты уполномоченных поставщиков интернет-услуг хостинга сайтов и электронной почты, иные ограничить.

Перечень уполномоченных поставщиков интернет-услуг хостинга сайтов и электронной почты утвержден приказом Оперативно-аналитического центра при Президенте Республики Беларусь 17.12.2010 г. № 92.

Для обеспечения должного уровня контроля за соблюдением работниками политики информационной безопасности:

- ознакомить всех сотрудников, имеющих доступ к локальным вычислительным сетям и рабочим местам (*ПЭВМ*) с выходом в сеть Интернет, с разработанной (*переработанной*) и утвержденной руководством политикой безопасности;
- провести инструктаж работников о недопущении открытия «зловредных ссылок» и вложений, полученных от неизвестных отправителей, при использовании корпоративных почтовых ящиков на

рабочих местах с доведением признаком подобных сообщений для их идентификации работниками;

- при увольнении работников предприятия, организации (*не зависимо от обстоятельств прекращения трудовых отношений*) принимать меры по смене логинов и паролей ото всех ранее предоставленных учётных записей (на ПЭВМ, на серверном оборудовании, учетные записи эл.почты, личных кабинетов организации и т.п.) в кратчайшие сроки, которые в зависимости от категории и направления деятельности предусмотреть политикой информационной безопасности. Факт смены реквизитов учётных записей ответственным специалистом отражать документально (*запись в журнале, акт и т.п.*);

- провести ревизию договорных отношений с обслуживающими (*поддерживающими*) программное обеспечение и официальные сайты коммерческими организациями в целях обеспечения качественности оказываемых услуг и надлежащего исполнения обязательств сторонами. В контексте данного мероприятия:

- проработать вопрос (*с привлечением компетентных специалистов, в т.ч. со стороны*) оптимальной частоты обновлений версий программных продуктов, программного обеспечения и платформ сайтов;

- инициировать (*в случае необходимости*) внесение в существующие договора изменений в части возложения обязанностей по контролю за своевременным техническим обслуживанием (конкретизировав мероприятия и сроки их выполнения), включая обновления ПО и платформ сайтов, а также ответственность за их неисполнение;

- организовать ведение учёта (*электронного, бумажного*) по работам, выполненным привлекаемыми фирмами, с целью контроля и принятия мер реагирования;

- не допускать случаев, когда доступ к панели управления хостингом и сайтом (логины и пароли) имеет только организация-исполнитель, и обеспечить хранение реквизитов доступа на бумажном носителе в сейфе;

- применять дополнительные меры по ограничению доступа к средствам администрирования платформы и сайта (перечень статических IP-адресов, доступ посредством VPN-клиента) и контролировать их актуальность.

Дополнительные мероприятия, направленные на повышение уровня информационной безопасности.

Ввести квалификационные требования к ответственным за обслуживание ЛВС и корпоративных сайтов специалистам, в соответствии с которыми осуществлять назначение на указанные должности лиц. Проводить регулярное повышение квалификации.

С учётом наличия финансовых ресурсов организовать закупку современного серверного оборудования (*межсетевых экранов*).

При выполнении перечисленных требований следует также руководствоваться мерами по обеспечению защиты общедоступной информации в информационных системах, разработанными Оперативно-аналитическим центром при Президенте Республики Беларусь, и размещенными в открытом доступе в сети Интернет:

https://www.oac.gov.by/recommendations-for-government-agencies