УТВЕРЖДЕНО
Приказом №84 от 25.12.2024г.

ПОЛИТИКА
Информационной безопасности
в УПП «Витебская областная типография»

Политика информационной безопасности определяет основы сетевой политики и информационной компьютерной безопасности, порядок доступа и правила работы пользователей персональных компьютеров с ресурсами локальной сети и глобальной компьютерной сети Интернет в УПП «Витебская областная типография» (далее – типография).

Настоящая Политика разработана с учетом требований Конституции Республики Беларусь, законодательных и иных нормативных правовых актов Республики Беларусь в области защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Система информационной безопасности в типографии как организованная совокупность специальных средств, методов и мероприятий, предназначена для:

- прогнозирования, своевременного выявления и устранения угроз профессионально значимым ресурсам и информационным системам типографии на основе правовых, организационных и инженерно-технических мер, а также средств обеспечения защиты;
- минимизации ущерба и оперативного восстановления программных и аппаратных средств, информации, пострадавших в результате кризисных ситуаций, выявление причин возникновения таких ситуаций и принятие соответствующих мер по их предотвращению;
- идентификации и регламентации доступа к сетевым ресурсам, в том числе к ресурсам глобальной компьютерной сети Интернет;

- предотвращения критических последствий несанкционированного распространения, уничтожения, искажения, копирования данных.

1.2. Положения Политики доводятся до ознакомления и являются обязательными для работников структурных подразделений типографии, организующихи обеспечивающих эксплуатацию информационных систем при выполнении своих служебныхобязанностей, физическихили юридических лиц, выступающих в качестве информационных посредников, операторов информационных систем и связи.

ГЛАВА 2 ОРГАНИЗАЦИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Организация и обеспечение эффективности функционирования системы информационной безопасности в типографии возлагаются на администратора сети.

2.2. Администратор сети обязан:

- обеспечивать бесперебойную работу основных сетевых сервисов, производить необходимые настройки и корректировки серверного программного обеспечения;
- осуществлять регулярный мониторинг параметров состояния локальной сети, обеспечивать ее бесперебойное функционирование;
- выполнять установку и регулярное обновление антивирусных программ, иных программных средств, необходимых для безопасного доступа к глобальной компьютерной сети Интернет;
- тестировать рабочие станции локальной сети на предмет наличия вредоносных программ;
- консультировать и осуществлять техническую поддержку пользователей по вопросам использования сетевых ресурсов и сервисов;
- сообщать руководству о выявленных фактах применения пользователями программных продуктов, приводящих к сбоям в работе компьютерного и/или сетевого оборудования, предназначенных для несанкционированного доступа, модификации, разрушения информационных ресурсов.

ГЛАВА 3 ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Внешний и VPN каналы передачи данных предоставляются типографии на договорной основе через провайдера, имеющего государственные лицензии на осуществление соответствующих видов

деятельности с учетом всех требований законодательства, в том числе требований информационной безопасности.

3.2. Персональные компьютеры закрепляются в помещениях типографии за строго определенными рабочими местами и идентифицируются в локальной сети на основании MAC адреса.

3.3. Идентификация пользователей сети обеспечена средствами операционных систем, установленных на устройствах пользователей. Аутентификация пользователей обеспечивается модулями авторизации информационных систем, используемых в типографии.

3.4. Обмен информацией между пользователями локальной сети осуществляется посредством сетевых дисков с настроенными правами доступа.

3.5. На серверах типографии настроен автоматизированный сбор и хранение информации о событиях информационной безопасности в виде протокола серверных логов, регистрирующих обращения к серверу и возникающие при этом ошибки, логи баз данных, фиксирующие запросы к базам данных, логи авторизации и аутентификации.

3.6. По мере необходимости обновляются операционные системы, корректируются методики использования серверного, системного и антивирусного программного обеспечения.

ГЛАВА 4 ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Сотрудники типографии имеют право:

- пользоваться локальными сетевыми ресурсами и ресурсами глобальной компьютерной сети Интернет для выполнения своих должностных обязанностей;
- обращаться за помощью к администратору сети по вопросам, возникающим при использовании сетевых ресурсов и сервисов;
- вносить предложения по улучшению работы сети.

4.2. Сотрудники типографии обязаны:

- соблюдать требования законодательства Республики Беларусь и настоящей Политики при работе с сетевыми информационными ресурсами;
- использовать ресурсы и сервисы глобальной компьютерной сети Интернет только для выполнения служебных обязанностей;
- использовать для обмена документами только официальные адреса электронной почты;
- при наличии ключей электронной цифровой подписи ЭЦП хранить их в недоступном месте, подключать их к компьютеру только на время работы с порталами требующими ЭЦП;

- блокировать доступ к компьютеру и служебным мобильным устройствам при уходе с рабочего места для предотвращения использования оборудования неавторизованными пользователями;

- уведомить администратора сети о случаях доступа третьих лиц к информационным системам типографии обусловленный производственной необходимостью;

- в случае обнаружения вредоносных программ, нестандартного поведения пользовательских приложений, возникновении нештатных ситуаций в работе компьютерных систем немедленно сообщать об этом администратору сети.

4.3. Сотрудникам типографии запрещается:

- допускать к работе за компьютером посторонних лиц, в том числе бывших работников типографии;

- изменять аппаратную конфигурацию оборудования, в том числе подключать нештатные устройства (флэш-диски, карты памяти, жесткие диски, мобильные телефоны и др.);

- устанавливать на компьютер и служебные мобильные устройства программное обеспечение, принимать предложения по обновлению программного обеспечения из непроверенных ресурсов глобальной компьютерной сети Интернет без согласования с администратором сети;

- использовать личные электронные почтовые ящики для осуществления деятельности типографии;

- при использовании электронных почтовых ящиков открывать сообщения от непроверенных адресатов, осуществлять рассылку спама;

- распространять в глобальной компьютерной сети Интернет непроверенные или заведомо ложные данные, информацию, унижающую честь и достоинство граждан, а также сведения служебного характера без разрешения руководителя.

Директор А.А.Бородий