УТВЕРЖДЕНО

приказ Средней школы № 5 г.Мозыря

01.07.2024 № 422

ПОЛИТИКА

г. Мозырь

 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ГЛАВА 1

ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности в государственном учреждении образования «Средняя школа № 5 г. Мозыря» (далее - Политика) определяет общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, в том числе и персональных данных.
2. 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.
3. Положения Политики служат основой для разработки локальных правовых актов, регламентирующих в государственном учреждении образования «Средняя школа № 5 г. Мозыря» (далее – учреждение образования) вопросы защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.
4. Ответственность за соблюдение информационной безопасности несет каждый работник учреждения образования.
5. В настоящей Политике под термином «работник» понимаются все работники учреждения образования.

ГЛАВА 2

НАЗНАЧЕНИЕ НАСТОЯЩЕЙ ПОЛИТИКИ

1. Повышение осведомленности работников в области рисков, связанных с информационными ресурсами учреждения образования.
2. Определение степени ответственности и обязанностей работников по обеспечению информационной безопасности в учреждении образования.
3. Обеспечение регулярного контроля за соблюдением положений настоящей Политики и проведение периодических проверок соблюдения информационной безопасности.

ГЛАВА 3

ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ

1. Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации учреждения образования. Соблюдение настоящей Политики обязательно для всех работников (как постоянных, так и временных).
2. Учреждению образования принадлежат на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления им деятельности в соответствии с действующим законодательством.
3. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования учреждения образования, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы учреждения образования.

ГЛАВА 4

ОБЩИЕ ПОЛОЖЕНИЯ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

1. Все работы в пределах помещений учреждения образования выполняются в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в учреждении образования.
2. Внос в помещения учреждения образования личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т. п.), а также вынос их за пределы учреждения образования производится только при согласовании с руководством учреждения образования.
3. В целях обеспечения санкционированного доступа к информационному ресурсу любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.
4. Работники учреждения образования должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования.

Не допускать хранение паролей к учётным записям в текстовых или иных файлах на локальных дисках.

Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

1. В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

ГЛАВА 5

ДОСТУП ТРЕТЬИХ ЛИЦ К ИНФОРМАЦИОННЫМ СИСТЕМАМ УПРАВЛЕНИЯ

1. Каждый работник обязан немедленно уведомить руководство учреждения образования обо всех случаях предоставления доступа третьим лицам к персональным носителям электронной информации.
2. Доступ третьих лиц к информационным системам учреждения образования должен быть обусловлен производственной необходимостью. В связи с этим порядок доступа к информационным ресурсам учреждения образования должен быть четко определен, контролируем и защищен.

ГЛАВА 6

УДАЛЕННЫЙ ДОСТУП

1. Работникам, использующим в работе портативные компьютеры учреждения образования, может быть предоставлен удаленный доступ к сетевым ресурсам учреждения образования в соответствии с правами в информационной системе учреждения образования.
2. Работникам, работающим за пределами учреждения образования с использованием компьютера, не принадлежащего учреждению образования, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.
3. Работники, имеющие право удаленного доступа к информационным ресурсам учреждения образования, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети учреждения образования и к каким-либо другим сетям, не принадлежащим учреждению образования.
4. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети учреждения образования, должны иметь программное обеспечение антивирусной защиты с последними обновлениями.

ГЛАВА 7

ДОСТУП К СЕТИ ИНТЕРНЕТ

1. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.
2. Рекомендованные правила:

24.1. работникам учреждения образования разрешается использовать сеть Интернет только в служебных целях;

24.2. запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения;

24.3. работа с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации учреждения образования в сеть Интернет за исключением размещения информации на официальном сайте, официальных страницах в Инстаграм, Телеграмм, чат-группах Viber в служебных целях;

24.4. работники учреждения образования перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

24.5. запрещен доступ в Интернет через сеть учреждения образования для всех лиц, не являющихся работниками учреждения образования, включая членов семьи работников учреждения образования.

ГЛАВА 8

ЗАЩИТА ОБОРУДОВАНИЯ

1. Работники должны обеспечивать физическую безопасность оборудования, на котором хранится информация учреждения образования.
2. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

ГЛАВА 9

АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

1. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы, дисководы для СD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы) для целей настоящей Политики вместе именуются компьютерным оборудованием.
2. Компьютерное оборудование, предоставленное учреждением образования, является его собственностью и предназначено для использования исключительно в служебных целях.
3. Пользователи портативных компьютеров, содержащих информацию учреждения образования, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства в случаях, когда данный компьютер не используется.

ГЛАВА 10

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

1. Все программное обеспечение, установленное на предоставленном учреждением образования компьютерном оборудовании, является собственностью учреждения образования и должно использоваться исключительно в служебных целях.
2. Работникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их служебной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено руководству учреждения образования.
3. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации.
4. Все компьютеры, подключенные к сети учреждения образования, должны быть оснащены системой антивирусной защиты.
5. Работники учреждения образования не должны:

34.1. блокировать антивирусное программное обеспечение;

34.2. устанавливать другое антивирусное программное обеспечение;

34.3. изменять настройки и конфигурацию антивирусного программного обеспечения.

ГЛАВА 11

РЕКОМЕНДУЕМЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Содержание электронных сообщений должно строго соответствовать стандартам учреждения образования в области деловой этики.
2. Строго конфиденциальная информация учреждения образования ни при каких обстоятельствах не подлежит пересылке третьим лицам по электронной почте.
3. Работникам учреждения образования запрещается использовать личные почтовые ящики электронной почты для осуществления деятельности учреждения образования.
4. Работники учреждения образования для обмена документами должны использовать только свой официальный адрес электронной почты.
5. В целях предотвращения ошибок при отправке сообщений работники перед отправкой должны внимательно проверить правильность написания имен и адресов получателей.
6. Недопустимые действия и случаи использования электронной почты:

40.1. поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

40.2. пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам учреждения образования в области этики.

1. Ко всем исходящим сообщениям, направляемым внешним пользователям, работник может добавлять уведомление о конфиденциальности.
2. Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в учреждении образования процедурами документооборота.

ГЛАВА 12

СООБЩЕНИЯ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

1. Работники обязаны уведомить директора или заместителей директора об известных или подозреваемых ими нарушениях информационной безопасности.
2. В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте руководству учреждения образования.
3. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан проинформировать руководство учреждения образования и (или) инженера-программиста для принятия мер по защите информации.
4. В случае установления факта нарушения политики информационной безопасности ответственному специалисту необходимо составлять докладную записку на имя директора школы.

ГЛАВА 13

ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

1. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах несут работники учреждения образования.
2. Необходимо регулярно делать резервные копии всех основных служебных данных.
3. Работники имеют право создавать, модифицировать и удалять файлы в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют разрешенный доступ.
4. Исключить возможность использования сторонних машинных носителей информации (флешки, жёсткие диски и т.д.) на рабочих местах без предварительной проверки содержимого на предмет вредоносного ПО.
5. Использовать сертифицированные ОАЦ РБ лицензионные антивирусные программные продукты.
6. Для обмена сведениями посредством Интернет-почты использовать только защищенные сервисы электронной почты уполномоченных поставщиков интернет-услуг хостингов сайтов и электронной почты, утверждённого приказом Оперативно-аналитического центра при Президенте Республики Беларусь 17.12.2010 №92.

ГЛАВА 14

ОТВЕТСТВЕННОСТЬЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ

1. Нарушение законодательства об информации, информатизации и защите информации влечет ответственность в соответствии с законодательными актами.

ПАМЯТКА

ОТВЕТСТВЕННОСТЬЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ

()

# Гл. 31 УК РБ Преступления против информационной безопасности

**Уголовный кодекс Республики Беларусь. Раздел XII. Глава 31. Преступления против информационной безопасности**

**Статья 349. Несанкционированный доступ к компьютерной информации.**

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, **– наказывается штрафом или арестом на срок до шести месяцев.**

2. То же действие, совершенное из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, – **наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.**

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, – **наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.**

**Статья 350. Модификация компьютерной информации.**

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации), – **наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.**

2. Модификация компьютерной информации, сопряженная с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, **– наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.**

**Статья 351. Компьютерный саботаж.**

1. Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж), **– наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.**

2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, – **наказывается лишением свободы на срок от трех до десяти лет.**

**Статья 352. Неправомерное завладение компьютерной информацией.**

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, – **наказываются общественными работами, или штрафом, или арестом на срок до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.**

**Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети.**

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети, **– наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.**

**Статья 354. Разработка, использование либо распространение вредоносных программ.**

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами, – **наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.**

2. Те же действия, повлекшие тяжкие последствия, – **наказываются лишением свободы на срок от трех до десяти лет.**

**Статья 355. Нарушение правил эксплуатации компьютерной системы или сети.**

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, – **наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.**

2. То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, – **наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.**

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, – **наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.**