Принято
Решением Общего собрания работников
ГБУ ЦДК Санкт-Петербурга
Протокол №1
От 20.06.2023

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 1B719B86CC617ECC61093D37D25D0E71
Владелец: Плетнева Евгения Борисовна
Действителен: с 07.04.2022 до 01.07.2023

Утверждаю:
Директор ГБУ ЦДК Санкт-Петербурга

_____
Е.Б. Плетнева

Приказ № 34-од от 20.06.2023

Порядок использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты в Государственном бюджетном учреждении Региональном центре психолого-педагогической, медицинской и социальной помощи «Центр диагностики и консультирования» Санкт-Петербурга (ГБУ ЦДК Санкт-Петербурга)

1. Общие положения

Порядок использования информационно-телекоммуникационных сетей международного информационного обмена и электронной почты в ГБУ ЦДК Санкт-Петербурга (далее – Порядок) разработан на основании Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации 05.12.2016 № 646, Специальных требований и рекомендаций по защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России 30.08.2002 № 282, Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и других нормативных правовых документов в области защиты информации.

Настоящий Порядок определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании информационно-телекоммуникационных сетей международного информационного обмена и электронной почты в ГБУ ЦДК Санкт-Петербурга.

Интернет - всемирная компьютерная сеть, которая использует для взаимодействия стек протоколов TCP/IP (протокол управления передачи сообщений / Интернет протокол). Работа в Интернет осуществляется в режиме реального времени (on-line). Существует ряд протоколов служб, связанных с TCP/IP и Интернетом. Наиболее распространенными из них являются:

- SMTP - протокол приема - передачи электронной почты.
- TELNET - протокол для подключения к удаленным системам, присоединенным к МИС общего пользования в режиме удаленного терминала.
- FTP - протокол, предназначенный для передачи файлов с одного компьютера на другой в вычислительной сети.
- DNS - служба сетевых имен, используемых для протоколов TELNET, FTP и т.д.
- WWW - служба (всемирная паутина), использующая гипертекстовый формат HTML (язык разметки гипертекста), предназначенная для передачи текстовой, графической, аудио и видео информации, а также ссылок на другие документы (гипертекстовые ссылки - выделенные области документа, позволяющие переходить к другому документу, содержащему связанную информацию).

Помимо перечисленных существует ряд служб и протоколов для удаленной печати, предоставления удаленного доступа к файлам и дискам, работы с распределенными базами данных и т.д.

Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах.

2. Источники угроз информационной безопасности

Подключение средств вычислительной техники к информационно-телекоммуникационным сетям международного информационного обмена представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (далее - НСД) в автоматизированные системы (далее - АС).

Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:

- проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;
- перенос в АС разрушающего программного обеспечения (внедрение программных закладок, вирусов);
- выбор и использование законным пользователем системы неудачных паролей;
- несанкционированная передача служебной информации ограниченного распространения пользователями в международные информационные сети (далее - МИС) общего пользования и т.д.

При непосредственном подключении локальной вычислительной сети к МИС общего пользования любой пользователь МИС имеет возможность:

- получить информацию об адресной структуре сети;
- установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);
- получить информацию о пользователях сети;
- попытаться подключиться к информационным ресурсам сети;
- вызвать отказ в обслуживании легальных пользователей.

Кроме явных, то есть непосредственно направленных на сеть органа внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением зловредного программного кода самими сотрудниками органа. К зловредному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов.

По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное использование модемов, подключенных к рабочим станциям пользователя. Причем подключение не обязательно может использоваться для доступа в Интернет (возможны соединения к серверам других организаций и к отдельным компьютерам, например, домашним).

3. Технические средства защиты информации

К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет, относятся:

- системы разграничения прав доступа;
- межсетевые экраны;
- системы построения защищенных виртуальных сетей (Virtual Private Network -VPN);
- системы обнаружения атак;
- системы анализа защищенности;

- системы антивирусной защиты и т.д.

Система разграничения доступа запрещает посторонним лицам доступ к ресурсам автоматизированной системы и позволяет разграничить права пользователей при работе на компьютере, при этом контролируются права локальных, удаленных и терминальных пользователей.

Межсетевой экран (далее - МЭ) представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Межсетевые экраны позволяют осуществить:
- контроль доступа на межсетевом уровне;
- протоколирование информационных потоков;
- сокрытие топологии защищаемой сети;
- реагирование на несанкционированные действия.

Средствами МЭ могут быть выявлены следующие виды атак:
- сканирование сетевых портов;
- атаки на отказ в обслуживании;
- изучение топологии внутренней сети;
- использование слабостей протоколов прикладного уровня;
- распространение вирусов и спама.

К дополнительным службам МЭ относятся:
- средства резервного копирования и восстановления;
- средства обеспечения высокой доступности;
- сетевая служба имен (split DNS).

Основные показатели защищенности МЭ:
- управление доступом;
- идентификация и аутентификация;
- регистрация событий и оповещение;
- контроль целостности;
- восстановление работоспособности.

Системы построения защищенных виртуальных сетей позволяют организовать прозрачное для пользователей соединение локальных вычислительных сетей с помощью шифрования.

К системам обнаружения атак можно отнести: системы обнаружения атак на уровне сети, системы обнаружения атак на уровне хоста. Системы обнаружения атак используют:

- системы обнаружения аномального поведения пользователя (большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, использование периферийных устройств, которые обычно пользователем не используются и т.д.);

- системы обнаружения злоупотребления (обнаружение уже известной атаки по шаблону или «сигнатуре»).

Средства анализа защищенности предназначены для поиска в вычислительной технике и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак.

4. Работа в сети Интернет

4.1. Доступ к сети Интернет для сотрудников ГБУ ЦДК Санкт-Петербурга предоставляется в рамках выполнения должностях инструкций и только на выделенных для работы с Интернет ресурсом персональных компьютерах.

4.2. Пользователи используют поиск информации в сети Интернет только в случае, если это необходимо для выполнения своих должностных обязанностей.

4.3. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом, могут быть запротоколированы и использоваться для принятия решения о применении к нему санкций.

4.4. Сотрудникам, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим или нарушает действующее законодательство Российской Федерации.

4.5. При необходимости переноса рабочих материалов, полученных из сети Интернет, на персональный компьютер пользователя, требуется их проверка при помощи антивирусных программ согласно Инструкции по организации антивирусной защиты в ГБУ ЦДК Санкт-Петербурга.

4.6. Сотрудники должны соблюдать настоящую Инструкцию после предоставления им доступа к сети Интернет.

5. Порядок осуществления доступа и обмена данными с внешними информационными ресурсами и по электронной почте

Установка и настройка программного обеспечения для работы с электронной почтой или ресурсами сети Интернет осуществляется администратором безопасности с привлечением сотрудников организации, обслуживающей вычислительную технику. Пользователям запрещается изменение любых параметров, касающихся способов подключения и используемых протоколов.

5.1. При работе с электронной почтой или ресурсами сети Интернет пользователям запрещается:

- обмен информацией для служебного пользования, а также информацией ограниченного доступа по электронной почте или с использованием ресурсов сети Интернет без использования средств криптографической защиты информации;
- использование ресурсов сети Интернет для развлечения и получения информации, не относящейся к функциональным обязанностям пользователя;
- предоставление доступа к электронной почте или к ресурсам сети Интернет с использованием данных своей учетной записи другим лицам;
- публикация своего служебного адреса электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей;
- подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением пользователем должностных обязанностей;
- открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением.

5.2.Электронная почта предоставляется сотрудникам только для выполнения своих прямых служебных обязанностей по заданию директора ГБУ ЦДК Санкт-Петербурга. Использование ее в личных целях запрещено.

5.3. ГБУ ЦДК Санкт-Петербурга оставляет за собой право получить доступ к электронной почте сотрудников, если на то будут веские причины.

5.4. Выходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение безопасности.

5.5. Пользователи не должны позволять кому-либо посылать письма от чужого имени.

6. Ответственность

6.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники.

6.2. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в сети и за ее пределами.

6.3. За нарушение настоящей Порядка пользователь может быть отстранен от работы в сети.