Частное образовательное учреждение
дополнительного профессионального
образования
ИНСТИТУТ ПРОМЫШЛЕННОЙ БЕЗОПАСНОСТИ, ОХРАНЫ ТРУДА И СОЦИАЛЬНОГО ПАРТНЕРСТВА
(Институт)

14.09.2015г. № 09/4

УТВЕРЖДАЮ
Директор Института
_____ Б.В.Егоров
«14» сентября 2015 г.

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ РАБОТ ПО ЭКСПЛУАТАЦИИ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ И ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение устанавливает порядок организации работ по техническому и технологическому обеспечению эксплуатации корпоративной компьютерной сети и обеспечению информационной безопасности при работе в корпоративной сети, права, обязанности и ответственность структурных подразделений, филиалов, представительств и сотрудников (далее - Сотрудники).

1.2. Требования настоящего Положения обязательны для исполнения при организации работ по техническому и технологическому обеспечению эксплуатации корпоративной компьютерной сети и обеспечению информационной безопасности при работе в корпоративной сети.

1.3. Данное положение разработано с учётом требований по обеспечению целостности и конфиденциальности информационной структуры и содержания компьютерных баз и банков данных, повышения эффективности работы средств информационной безопасности предприятия, выполнения требований ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» и ГОСТ Р ИСО/МЭК 17799 – 2005 "Информационная технология. Практические правила управления информационной безопасностью"

1.4. Термины и определения, применяемые в настоящем Положении:

Корпоративная компьютерная сеть (ККС) – совокупность технических устройств (рабочие станции, компьютеры, принтеры, факсы, телефонные аппараты, сканеры) и коммуникационного оборудования (машрутизаторы, кабельные сети), объединенных в единую систему цифровой обработки информации.

Техническое обеспечение ККС - обеспечение рабочих мест структурных подразделений стационарно установленными, переносными и портативными техническими устройствами, предназначенными для работы с информационными ресурсами, доступными в ККС.

Технологическое обеспечение ККС – обеспечение построения распределённой компьютерной сети, прокладка и установка коммуникационного оборудования, настройка протоколов обмена информацией, организация программно-аппаратного доступа в глобальную информационную сеть Интернет. Подключение к сети необходимого технического оборудования, установленного на рабочих местах в

структурных подразделениях. Применение современных информационных технологий в обеспечении информационной безопасности.

Программное обеспечение – комплект компьютерных программ, обеспечивающий бесперебойную работу технических устройств ККС в рамках задач, решаемых на конкретном рабочем месте.

Информационная безопасность – целенаправленная деятельность структурных подразделений и должностных лиц с использованием разрешенных сил и средств по достижению состояния защищённости информационной среды, по предотвращению утечки защищаемой информации, несанкционированных и преднамеренных воздействий на защищаемую информацию, проникновения вредоносной информации в ККС.

2. ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ККС.

2.1. Управление информационных технологий:

2.1.1. Ведёт планирование приобретения и использования, а также учет технических устройств, используемых в ККС, выполняет техническое обслуживание с целью поддержания исправного состояния технических устройств.

2.1.2. Обеспечивает установку на рабочие места необходимых технических устройств по заявкам руководителей структурных подразделений, директоров филиалов и представительств.

2.1.3. Обеспечивает установку необходимого программного обеспечения на технические устройства.

2.1.4. Организует техническую поддержку устройств в ККС в режиме реального времени (тел. (812)702-6220).

2.1.5. Организует и осуществляет контроль за использованием технических устройств.

2.1.6. Выдает рекомендации о необходимости замены технических устройств в ККС в связи с развитием ПО или изменением функциональных нагрузок.

2.1.7. Организует работы по перемещению или развитию ККС.

2.1.8. По заявке руководителей структурных подразделений, директоров представительств организует выделение виртуальных областей на сетевых ресурсах для хранения данных.

2.2. Руководители структурных подразделений, директора филиалов и представительств:

2.2.1. Организуют оснащение рабочих мест сотрудников необходимыми техническими устройствами, обеспечивают оформление заявок на установку необходимых технических устройств и программного обеспечения

2.2.2. Обеспечивают безопасную эксплуатацию технических устройств, работающих в ККС, установленных на рабочих местах сотрудников.

2.2.3. Организуют обучение сотрудников применению и правилам безопасной эксплуатации технических устройств ККС.

2.2.4. Организуют своевременное оформление заявок на необходимое программное обеспечение технических устройств, установленных на рабочих местах сотрудников.

2.2.5. Несут ответственность в установленном порядке за установку несанкционированного и вредоносного ПО, за сохранность всех данных, хранящихся в технических устройствах, установленных на рабочих местах.

3. ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ККС.

3.1. Управление по развитию информационных технологий:

3.1.1. Руководитель Центра цифровых технологий выполняет функции системного администратора и IT директора.

3.1.2. Обеспечивает работу иерархической структуры ККС.

3.1.3. Организует работу пользовательских сервисов ККС.

3.1.4. Определяет права доступа к общим ресурсам и ресурсам Internet с рабочих мест ККС в соответствии с заявкой от руководителей структурных подразделений.

3.1.5. Организует и определяет порядок доступа к ресурсам ККС внешних пользователей (сайт, дистанционная подготовка и т.п.)

3.1.6. Обеспечивает применение новейших информационных технологий для обеспечения конфиденциальности информации, хранящейся в технических устройствах ККС.

3.1.7. Организует резервное копирование данных, хранящихся на сетевых устройствах в ККС.

3.2. Руководители структурных подразделений, директора филиалов и представительств:

3.2.1. Определяют состав данных, подлежащих резервированию, и порядок доступа к ним.

3.2.2. Подают заявку на создание сетевого ресурса в которой указывают:

- Название сетевой папки
- Имена пользователей, имеющих доступ к сетевой папке

4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Управление информационных технологий и Управление по развитию информационных технологий:

4.1.1. Обеспечивают комплекс мероприятий с использованием разрешенных сил и средств по достижению состояния защищённости информационной среды, по предотвращению утечки защищаемой информации, несанкционированных и преднамеренных воздействий на защищаемую информацию, проникновения вредоносной информации в ККС.

4.1.2. Обеспечивают возможность ограничения (по согласованию с директором) доступа к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а так же к ресурсам, содержание и направленность которых запрещены международным и российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.

4.2. Руководители структурных подразделений, директора филиалов и представительств:

4.2.1. Обеспечивают комплекс мероприятий с использованием разрешенных сил и средств по достижению состояния защищённости информационной среды, по предотвращению утечки защищаемой информации, несанкционированных и преднамеренных воздействий на защищаемую информацию, проникновения вредоносной информации в ККС.

4.2.2. Обеспечивают комплекс мероприятий, направленных на **запрещение:**

- установки на рабочие станции несанкционированного ПО;
- разглашения коммерческой и служебной информации, ставшей известной сотруднику по служебной необходимости либо иным путем;
- распространения защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;
- публикации, загрузки и распространения материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию;
- распространения информации ресурсов, содержание и направленность которых запрещены международным и российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.
- загрузки и запуска исполняемых либо иных файлов без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
- использование анонимных прокси серверов.

4.2.3. При работе с корпоративной электронной почтой обеспечивают комплекс мероприятий, направленных на **запрещение:**

- публикации своего адреса, либо адреса других сотрудников на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- массовой рассылки почтовых сообщений рекламного характера без предварительного согласования с заместителем директора по информационным технологиям.
- распространения информации ограниченного доступа;
- предоставления, кому бы-то ни было пароля доступа к своему почтовому ящику
- открытия писем из непонятных источников и переход по ссылкам, указанным в теле письма или вложении.

Зам. директора В.Н. Дранишников

Зам. директора Д.Л. Миньков