

ЭН+ ХОЛДИНГ ЛИМИТЕД
Россия, 121096, Москва
ул. Василисы Кожиной, д.1
Тел: +7 (495) 642 7937
Факс: +7 (495) 642 7938
www.enplusgroup.com

EN+ HOLDING LIMITED
1 Vasilisy Kozhinoy St.,
Moscow, 121096, Russia
Tel.: +7 (495) 642 7937
Fax: +7 (495) 642 7938
www.enplusgroup.com



УТВЕРЖДЕНЫ
Приказом от 30.10. 2020 г.
№ ЭНГ-П-20-021

**Правила пользования средствами ЭВТ, оргтехники
и информационными ресурсами при работе
в корпоративной информационно-вычислительной сети
(далее – Правила)**

1 Введение

1.1 Назначение

1.1.1 Действие настоящих Правил направлено на обеспечение необходимой эффективности, надёжности и бесперебойности работы средств электронно-вычислительной техники и оргтехники, штатного функционирования корпоративных сервисов электронной почты, баз данных, доступа в Интернет, экономного использования телекоммуникационных ресурсов, а также. на повышение безопасности хранения, обработки и передачи информации, за счёт соблюдения установленных требований.

1.1.2 Настоящие Правила определяют обязанности, права и ответственность пользователя автоматизированного рабочего места во время работы в корпоративной информационно-вычислительной сети при обработке, хранении и передаче информации.

1.2 Термины и сокращения

В настоящих Правилах используются следующие термины и сокращения:

№	Термин/сокращение	Определение
1.	Владелец информационного ресурса	Должностное лицо, исполняющее обязанности руководителя структурного подразделения, наделенное правами владения и ответственностью в отношении информационного ресурса в полном или ограниченном объеме.
2.	Группа Эн+	Группа юридических лиц, связанных отношениями экономической и корпоративной зависимости.
3.	Доступ к информационному ресурсу	Возможность получения и обработки данных, составляющих информационный ресурс.
4.	Информация	Сведения (сообщения, данные) независимо от формы их представления.
5.	Информационная безопасность Компании (ИБ)	Состояние защищенности информации и информационных ресурсов, при которых обеспечивается конфиденциальность, целостность и доступность информационных ресурсов

№	Термин/сокращение	Определение
		(активов) предприятия, а также аутентичность данных и апеллируемость.
6.	Информационная система	Совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации с целью решения бизнес-задач подразделений Компании.
7.	Информационный ресурс	Информация в электронном виде, доступная посредством именованного раздела, включающая в себя прикладное, системное программное обеспечение (ПО), прикладные системные данные, обеспечивающие функционирование прикладных задач.
8.	Исполняемый файл	Файл, содержащий в себе программный код, который запускается при его открытии.
9.	Ключ доступа	Переносное устройство, содержащее уникальную последовательность символов, предназначенное для удостоверения личности владельца.
10.	Компания	ФЧК ОО «Эн+ Холдинг Лимитед», а также партнеры, являющиеся пользователями или администраторами информационных систем Группы Эн+ и подписавшие соответствующие соглашения юр. лица.
11.	Конфиденциальность информации	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
12.	Корпоративная информационно-вычислительная сеть (КИВС)/ Корпоративная сеть	Объединение информационных систем, компьютерного, телекоммуникационного оборудования всех подразделений Компании посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи.
13.	Подразделение по информационным технологиям (ИТ Служба)	Подразделение Компании, осуществляющее функции ИТ обеспечения Компании, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.
14.	Подразделение по информационной безопасности (ИБ)	Подразделение (работник) Компании, ответственное за контроль обеспечения информационной и кибербезопасности Компании, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.
15.	Пользователь	Сотрудник Компании либо иное лицо, зарегистрированное в корпоративной информационно-вычислительной сети, использующее информационные ресурсы Компании для выполнения своих должностных обязанностей или договорных обязательств.
16.	АРМ	Автоматизированное рабочее место
17.	ИБ	Информационная безопасность
18.	ИТ	Информационные технологии
19.	ПО	Программное обеспечение
20.	ПК	Персональный компьютер
21.	КЭП	Корпоративная электронная почта
22.	ЭВТ	Электронно-вычислительная техника
23.	ЭП	Электронная подпись

2 Основные положения

2.1. Вся информация, создаваемая, хранимая, обрабатываемая и передаваемая по каналам связи в корпоративной сети Компании и с использованием оборудования принадлежащего Компании, которая не была специально идентифицирована как собственность третьих сторон, является собственностью Компании и называется «служебной информацией».

2.2. Служебная информация Компании (включая финансовые электронные документы, базы данных, сообщения электронной почты, списки рассылки, техническую документацию и т.п.) должна использоваться только в производственных целях. Границы допустимого использования этой информации определяет руководство Компании. Использование служебной информации в любых других целях, включая публикации в специальной или учебной литературе, в сети Интернет и т. п., допускается только по согласованию с руководством Компании.

2.3. Допуск Пользователей к корпоративным информационным ресурсам и сетевым сервисам осуществляется только после ознакомления с настоящими Правилами, на основании направления типовых заявок в подразделение по информационным технологиям, после согласованию руководителя соответствующего структурного подразделения и владельца информационного ресурса, а также подразделения ИБ.

2.4. Контроль за соблюдением Пользователем требований настоящих Правил осуществляется руководителем его подразделения, ИТ Службой и Подразделением ИБ.

3 Правила использования средств ЭВТ и оргтехники

3.1 Пользователь имеет право на:

3.1.1 Пользование средствами ЭВТ, оргтехники и информационными ресурсами Компании, необходимыми для выполнения служебных обязанностей.

3.1.2 Использование штатного программного обеспечения, установленного специалистами ИТ службы. Программное обеспечение подразделяется на устанавливаемое в обязательном порядке и устанавливаемое по запросу Пользователя (Опциональное ПО). Установка опционального ПО осуществляется по отдельному согласованию, при условии соблюдения лицензионных требований по использованию ПО.

3.1.3 Обеспечение сохранности служебной информации, размещённой на корпоративных файловых хранилищах, и восстановлении данных в случае сбоя.

3.1.4 Получение консультаций по работе со средствами ЭВТ, оргтехникой и по работе в Корпоративной сети от специалистов ИТ Службы и подразделения ИБ

3.1.5 Использование ресурсов глобальных телекоммуникационных сетей (Интернет), если выполнение должностных обязанностей без этого невозможно;

3.2 Пользователь обязан:

3.2.1. Использовать выделенные средства ЭВТ, информационные ресурсы, программное обеспечение и оргтехнику исключительно в служебных целях.

3.2.2. Обеспечивать конфиденциальность ключей доступа, паролей к информационным ресурсам и системам.

3.2.3. Соблюдать требования парольной политики Компании:

- минимальная длина пароля 8 символов;
- в составе пароля должны присутствовать три группы символов из четырех: строчные буквы (a-z, a-я), заглавные буквы (A-Z, A-Я), цифры и специальные символы (точки, тире, нижние подчёркивания, запятые и т.п.);
- пароли не должны включать в себя легко вычисляемые сочетания символов (имена, фамилии, дата рождения, наименование отделов и т.п.), общепринятые сокращения, имена учетных записей;
- пароли не должны являться персональной информацией (имена членов семьи, адреса, телефоны, даты рождения и т.п.);

– сотрудник обязан выполнять смену пароля при первичной регистрации в сети или в Информационной системе, а также немедленно, по требованию подразделения ИТ или ИБ¹;

– сотрудник обязан выполнять плановую смену пароля не реже 1 (одного) раза в 3 (три) месяца. При этом новый пароль не должен повторять 10 (десять) предыдущих паролей;

– при вводе пароля необходимо исключить возможность его зрительного фиксирования посторонними лицами.

3.2.4. Сохранять и поддерживать в актуальном состоянии служебную информацию, связанную со своей деятельностью, в персональной папке (либо папке отдела) на выделенном корпоративном файловом сервере. Помнить, что данные, хранимые на локальной рабочей станции (папки «Мои документы», «Рабочий стол» и др.), в отличие от данных на сетевом диске, не подлежат периодическому резервному копированию и в случае технического сбоя, могут быть утеряны безвозвратно. Размещение файлов в сетевой персональной папке это ответственность каждого сотрудника и если данные утрачены, а копии на сетевой папке нет, то ответственность лежит на сотруднике.

3.2.5. Рационально использовать ресурсы сетевых папок, своевременно производить удаление служебной информации, потерявшей актуальность или устаревшей.

3.2.6. Блокировать работу своего АРМ в период отсутствия на своём рабочем месте²

3.2.7. Контролировать документы, выводимые на печать, не допускать несанкционированного доступа к распечатанной информации в процессе и после печати.

3.2.8. Прекращать работу в сети (с определённым сетевым сервисом или ресурсом) по требованию подразделения ИТ или ИБ.

3.2.9. Ежедневно производить перезагрузку рабочего компьютера для своевременного обновления системного программного обеспечения³.

3.3 Руководители подразделений и служб дополнительно обязаны:

3.3.1. Ознакомить подчинённых с настоящими Правилами под роспись.

3.3.2. Передать подписанные листы ознакомления в кадровую службу, для хранения наряду с личными делами (на случай судебных споров). Копия листа ознакомления сохраняется в подразделении на весь период работы сотрудника.

3.3.3. При увольнении/переводе подчинённых обеспечить необходимые меры к предотвращению утечки информации, такие как:

- подать заявку в подразделение по информационным технологиям о блокировании доступа в Интернет к переносным устройствам информации, внешней электронной переписке и к удалённому доступу для увольняемого сотрудника. Если дата увольнения известна заранее – то не менее чем за 3 дня до неё, в ином случае – сразу после получения соответствующей информации;⁴
- в день увольнения сотрудника выполнить смену паролей и ключей доступа, которые могли быть известны уволенному. При невозможности быстрой смены, согласовать с подразделением ИБ план по замене;
- при необходимости сохранения данных сотрудника или передачи их другому лицу подать заявку об этом в ИТ службу до фактической даты увольнения (согласование подразделения ИБ обязательно);

¹ Смена пароля производится путем нажатия на клавиатуре Ctrl+Alt+Del либо Ctrl+Alt+End и пункт «Изменить пароль»

² Используя комбинацию Ctrl+Alt+Del и пункт «Блокировка» или комбинацию клавиш Win+L.

³ Кроме случаев, согласованных с подразделением ИБ, когда ПК обеспечивает непрерывность технологического процесса или других бизнес-задач.

⁴ В случаях, когда дата неизвестна заранее, эти действия следует предпринять сразу после получения информации об увольнении сотрудника.

- при переводе сотрудника на новую должность или в другое подразделение – подать заявку в ИТ службу с корректировкой доступа (прекратить доступ к ресурсам которые уже не будут необходимы сотруднику для работы).

3.4 Пользователю запрещается:

3.4.1. Передвигать оргтехнику во время работы во включённом состоянии (кроме мобильных ПК).

3.4.2. Самостоятельно производить действия, связанные с⁵:

- разборкой (вскрытием корпуса) и модернизацией;
- подключением/отключением периферийного оборудования к ПК (исключения составляют сотрудники мобильных ПК при работе с выданным им ИТ Службой периферийным оборудованием);
- установкой или удалением программного обеспечения;⁶
- запуском исполняемых файлов, не входящих в штатное программное обеспечение (см. п. 3.1.2 настоящих Правил);
- подключениями/отключениями к сетевым разъёмам и портам локальной сети (кроме сотрудников, работающих с мобильными ПК);
- подключением/отключением устройств, создающих каналы связи (модем, мобильные устройства, Wi-Fi/Bluetooth адаптеры) без согласования с ИБ;
- изменениями параметров настроек антивирусных пакетов, программ, системных настроек операционной системы (включая манипуляции с реестром, разрешениями на системные папки операционной системы, копированием исполняемых файлов, изменениями в уровнях доступа к компьютеру, изменениями или фальсификация журналов регистрации событий, сервисов и т.п.);
- подключением любых носителей информации (флешки, компакт-диски, дискеты, мобильные телефоны, планшеты и пр.) к компьютеру без получения предварительного разрешения на такого рода действия от непосредственного руководителя и согласования со стороны подразделения ИБ.

3.4.3. Ограничивать и/или изменять параметры доступа, менять/создавать сетевой доступ к информационным ресурсам без согласования со стороны подразделения ИБ.

3.4.4. Сообщать персональные реквизиты доступа (имя/пароль) к сетевым ресурсам (учётной записи, базам данных, другим ресурсам КИВС), передавать ключи доступа иным лицам (включая других сотрудников Компании или ИТ Службы) без согласования с подразделением ИБ.

3.4.5. Предпринимать попытки или осуществлять доступ к чужим данным или сетевым ресурсам под чужим персональными реквизитами доступа (сетевым именем и паролем) без согласования со стороны подразделения ИБ.

3.4.6. Размещать информацию неслужебного характера в папках на ПК и серверах.

3.4.7. Копировать служебную информацию в пределах Компании, используя личные носители информации, при наличии других возможностей переноса информации (таких как сетевые папки, электронная почта, корп. портал и т.д.)⁷.

3.4.8. Использовать для обмена служебной информацией и ведения переписки средства электронной почты, не являющиеся корпоративными, и личные почтовые ящики, зарегистрированные на общедоступных сервисах в сети Интернет.

⁵ Пункт не распространяется на специалистов службы по информационным технологиям, специалистов по информационной безопасности и иных специалистов осуществляющих поддержку информационных систем - при условии согласования со стороны подразделения ИБ.

⁶ Пункт не распространяется на приложения, распространяемые через центр программного обеспечения Microsoft System Center.

⁷ Прежде чем воспользоваться внешними носителями информации для копирования данных следует убедиться, что исчерпаны другие способы переноса информации (сетевые папки, электронная почта, корп. портал). При необходимости проконсультироваться в подразделении ИТ или ИБ.

3.4.9. Регистрировать и использовать корпоративные адреса электронной почты для получения рассылок, не относящихся к служебной деятельности.

3.4.10. Копировать на личные носители информации служебную информацию для использования за пределами периметра КИВС без согласования с подразделением ИБ.

3.4.11. Разглашать, копировать на внешние носители, передавать по незащищённым каналам связи, пересылать конфиденциальную информацию. Передача конфиденциальной информации допускается только после согласования со стороны подразделения ИБ с соблюдением мер защиты (т.к. шифрование, архивация в формат 7Z с паролем, соответствующим требованию п. 3.2.3 и т.д.).

3.4.12. Распространять и копировать защищённые авторскими правами материалы, затрагивающие какой-либо патент, товарный знак (торговую марку), коммерческую тайну, авторские права (копирайт), смежные права или прочие права собственности и/или иные права третьих сторон.

3.4.13. Публиковать, загружать, запускать или распространять материалы, заведомо содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, программы для осуществления несанкционированного доступа, обхода авторской защиты ПО (генераторы лицензий, ключей и т.п.), лицензии и серийные номера.

3.5 **Правила поведения в нестандартных ситуациях:**

3.5.1. В случае возникновения признаков компрометации пароля либо несанкционированного доступа в отсутствие Пользователя необходимо немедленно сменить пароль и поставить в известность подразделение ИБ или ИТ.

3.5.2. При обнаружении компьютерных вирусов или возникновения характерных изменений при работе ПК (регулярные сбои, “зависания”, сильные замедления в работе), иных нарушений, замеченных в работе средств ЭВТ - немедленно обратиться к специалистам службы ИТ.

3.6 **Правила использования Корпоративной электронной почты.**

3.6.1 При использовании ресурсов КИВС или системы Корпоративной электронной почты (КЭП) пользователь соглашается с тем, что:

3.6.1.1 электронная переписка в Компании приравнивается к служебной и является допустимым доказательством при проведении расследований;

3.6.1.2 вся информация, принимаемая и отправляемая с использованием компьютеров Компании (в т.ч. посредством КЭП), является собственностью Компании и не считается персональной;

3.6.1.3 Компания вправе накапливать, отслеживать, уничтожать переписку в соответствии с решениями принимаемыми на уровне руководства Компании.

3.6.2 При использовании КЭП Пользователь обязан:

3.6.2.1 Соблюдать правила деловой этики/деловой переписки. Находясь на рабочем месте, не менее чем два раза за рабочий день обрабатывать полученную от партнёров, коллег и клиентов информацию.

3.6.2.2 Рационально использовать ресурсы КЭП. Передавать в одном почтовом отправлении файлы объёмом не более 30 мегабайт. При необходимости передачи файлов большего размера их следует разбить на части объёмом каждый не более максимального размера и передать несколькими сообщениями (письмами).

3.6.2.3 При получении в почтовом сообщении и в прикрепленных архивах исполняемых файлов (например, с расширением .bat, .bin, .com, .cmd, .exe, .hta, .jar, .js, .ps1, .scr, .vbs, .wsh), подозрительных вложений от неизвестных отправителей не открывать их и о факте получения такого почтового сообщения поставить в известность специалистов службы ИТ

и подразделения ИБ, а также отправить подозрительное сообщение с вложенным документом на специальный почтовый адрес, определенный в Компании службой ИТ и подразделением ИБ.

- 3.6.2.4 При получении писем, содержащих ссылки на внешние ресурсы, не переходить по указанным ссылкам, предварительно не убедившись в надежности источника. В случае сомнений поставить в известность службу ИТ или ИБ путём пересылки письма на специальный почтовый адрес, определённый в Компании службой ИТ и подразделением ИБ.
- 3.6.2.5 При открытии полученных по КЭП файлов документов формата MS Word, MS Excel с подключёнными к ним макросами не открывать полученный документ и связаться с службой ИТ (кроме случаев, когда надёжность отправителя не вызывает подозрений).
- 3.6.2.6 Сообщения, содержащие конфиденциальную информацию (согласно действующему СТП «Защита конфиденциальной информации»), отправлять только с использованием процедур защиты, согласованных с со стороны подразделения ИБ.
- 3.6.2.7 Перед отправкой электронного письма дополнительно сверять адресатов сообщения – убедиться, что все они указаны верно (в Компании много однофамильцев).
- 3.6.2.8 Использовать подпись в каждом сообщении с указанием следующих данных: фамилии, имени, отчества полностью, должности, контактного телефона.
- 3.6.2.9 Не превышать установленные ограничения размера почтового ящика, своевременно проводя архивирование и/или удаление старых почтовых сообщений.⁸

4 Использование глобальных сетей и Интернет

4.1 Общие положения

4.1.1 Доступ в глобальные сети, такие как Интернет, предоставляется сотрудникам Компании только для выполнения должностных обязанностей. Действия пользователей в сетях протоколируются. Пользуясь ресурсом, пользователь соглашается, что автоматические журналы регистрации доступа на серверах и в информационных системах имеют доказательный статус при проведении расследований.

4.1.2 Пользователь обязуется оптимально использовать пропускную способность каналов связи – передавать большие файлы в моменты наименьшей нагрузки. Если пользователь утилизирует большую часть канала, и это существенно снижает общую производительность – ИТ подразделение может временно отключать доступ пользователя.

4.2 При работе в глобальных сетях запрещено:

4.2.1. Использовать ресурсы для неслужебных целей.

4.2.2. Получать из Сети информацию, содержащую исполняемые модули, программы, драйвера и т.п. программное обеспечение без согласования с ИТ службой или подразделением ИБ.⁹

4.2.3. Использовать для передачи служебной информации сервисы публичных серверов: почтовых сервисов (таких как www.mail.ru, www.hotmail.ru и т.п.), видеосвязи и иных облачных сервисов (файлов, сообщений и т.д.), без согласования подразделения ИБ.

4.2.4. Использовать сторонние прокси-сервера и иные средства обхода блокировок доступа, без согласования с подразделением ИБ.

⁸ Сообщения старше 30 дней с момента создания/получения удаляются из почтового ящика автоматически.

⁹ Пункт не распространяется на специалистов службы по информационным технологиям, специалистов по информационной безопасности и иных специалистов, осуществляющих поддержку информационных систем - при условии согласования со стороны подразделения ИБ.

4.2.5. Публиковать материалы, содержащие серийные номера к коммерческим программам, программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещать ссылки на вышеуказанную информацию.

5 Правила удалённого доступа к ресурсам Компании

5.1 Общие положения

5.1.1 При наличии обоснования сотруднику может быть предоставлен удалённый доступ к ресурсам Компании (удалённый рабочий стол, доступ к почте с телефона и т.п.).

5.2 При наличии удалённого доступа пользователь обязан:

5.2.1 Самостоятельно решать вопросы безопасности и защищённости личного устройства (например, домашнего компьютера, планшета или мобильного телефона). В частности, ежедневно обновлять антивирусное программное обеспечение и не менее чем один раз в месяц устанавливать обновления системного программного обеспечения.¹⁰

5.2.2 Использовать для удалённого доступа личные устройства с операционными системами, не имеющими критических уязвимостей по безопасности и находящимися на поддержке производителя в части выпуска обновлений безопасности. При прекращении поддержки – прекратить использовать устройство.

5.2.3 Производить доступ с ограниченного числа устройств, не являющихся публичными. Обеспечивать физическую безопасность всех устройств от посягательства третьих лиц и невозможность считывания с них информации.

5.2.4 По требованию сотрудников подразделения ИБ предоставлять все сведения об устройстве, с которого осуществляется удалённый доступ. При подозрении на наличии проблем ИБ - предоставлять возможность проверки этого устройства на соответствие требованиям информационной безопасности Компании.

5.2.5 Понимать и принимать тот факт, что нарушения, допущенные при удалённом доступе, несут для Компании очень высокие риски. Передача пароля, нецелевое использование, халатность, приведшая к компрометации пароля и имени доступа - могут быть причиной финансовых и репутационных потерь для Компании. Подобные нарушения являются основанием для привлечения к дисциплинарной ответственности (вплоть до увольнения).

6 Правила работы с ключами электронной подписи

6.1 Пользователь обязан:

6.1.1 Обеспечивать физическую безопасность вверенных ему ключей доступа (такие как e-token, smart-карты, ЭП и иные переносные устройства, используемые при доступе к информации), не оставлять на рабочем месте без присмотра, при хранении в рабочем кабинете использовать только надёжные запираемые хранилища, доставая из хранилища только на период использования.

6.1.2 Уничтожать недействительные ключи доступа только согласно установленным нормам обращения с конфиденциальной информацией, СТП «Обеспечение информационной безопасности технических средств».

6.1.3 Незамедлительно сообщать в подразделение ИБ о случаях известной пользователю компрометации ключей ЭП и организовывать их блокировку.

6.1.4 По истечении срока действия ключей с периодичностью, установленной договорами и документацией, необходимо заблокировать и сменить ключи ЭП.

¹⁰ Сотрудники информационной безопасности могут дать заключение о безопасности устройства и наличии всех необходимых установленных компонент.

6.1.5 Ключи ЭП уничтожаются во всех случаях увольнения или смены владельца ЭП, за исключением случаев, когда ключ необходим для дешифрования архивной корреспонденции (по согласованию с подразделением ИБ).

6.1.6 В случае, если работа с ключом ЭП выполняется вместо владельца ЭП ответственным пользователем, данные функции закрепляются в должностной инструкции ответственного пользователя ЭП, оформляются доверенность на использование ключа ЭП и акт приема-передачи носителей с ключами ЭП по установленным формам.

6.1.7 При временном выполнении функций ответственного пользователя ключа ЭП другим лицом издается приказ Компании на исполнение обязанностей этим лицом и оформляется акт приема-передачи носителей с ключами ЭП. По факту завершения периода исполнения обязанностей, ключ с ЭП возвращается владельцу (с отметкой в акте), владелец ключа ЭП, по его возврату, обязан сменить пароль доступа к ключевой информации.

6.1.8 Руководитель подразделения, в котором эксплуатируется ключ доступа, проводит контроль оформления ответственными пользователями ключей ЭП доверенностей на использование ключей ЭП по установленной форме.

6.1.9 Если использование корпоративной ЭП согласовано на личном устройстве (мобильный телефон, планшет или компьютер), то при утере, выходе из строя или замене на новое личного устройства, сотрудник обязан информировать подразделение ИБ и получить новую ЭП. При этом старая ЭП добавляется в списки недействительных.

6.2 Пользователю запрещается:

6.2.1 Записывать на ключевые носители постороннюю информацию, использовать в качестве ключевых личные носители.

6.2.2 Снимать несанкционированные копии с ключевых носителей.

6.2.3 Знакомить с содержанием ключевых носителей или передавать конфиденциальную информацию (ключи, пароли и проч.) лицам, к ним не допущенным.

6.2.4 Знакомить с техническими и программными средствами системы, механизмами защиты третьих лиц.

7 Ответственность

7.1 За нарушение требований и положений настоящих Правил Пользователь может быть привлечен к дисциплинарной ответственности в соответствии с положениями действующего трудового законодательства.

7.2 Руководители структурных подразделений Компании несут ответственность за ознакомление под роспись подчинённых сотрудников с настоящими Правилами, а также за надлежащее выполнение подчинёнными сотрудниками положений настоящих Правил.

Лист ознакомления

С Правилами пользования средствами ЭВТ, оргтехники и информационными ресурсами при работе в корпоративной информационно-вычислительной сети, утвержденной приказом от _____.2020 № _____ ознакомлен:

Дата	Фамилия И.О.	Подпись

Руководитель подразделения

(инициалы, подпись).