АО «Газпром газораспределение Астрахань»

Группа по корпоративной защите

Памятка пользователю по информационной безопасности

Каждый пользователь локальной вычислительной сети (далее - ЛВС) АО «Газпром газораспределение Астрахань» (далее - Общество), участвующий в рамках выполнения своих служебных обязанностей в процессах обработки информации и имеющий доступ (в том числе полученный нелегально) к техническим средствам, программному обеспечению и информации Общества, несет персональную ответственность за свои действия и ОБЯЗАН:

- строго соблюдать установленные правила обеспечения информационной безопасности в Обществе при работе с программными и техническими средствами ЛВС.
- бережно относиться к используемым материальным ценностям и нематериальным ресурсам - не допускать нарушения работоспособности технических средств, программ, средств защиты, телекоммуникационных каналов и т.п., а также конфиденциальности, целостности и доступности обрабатываемых в них информации.
- информировать непосредственного руководителя структурного подразделения, Отдел информационных технологий и связи (далее – ОИТиС) или Группу по корпоративной защите (далее - ГКЗ) об обнаруженных нештатных ситуациях в ЛВС (отклонения в нормальной работе программных или технических средств, компрометация паролей, несанкционированное подключение устройств, вирусное заражение, разглашение информации ограниченного доступа, перебои в системе электроснабжения, проникновение на территорию посторонних лиц, опасность возгорания, затопления и т.п.).

Пользователю ЗАПРЕЩАЕТСЯ:

- использовать компоненты программных или технических средств ЛВС, а также служебную информацию в неслужебных (личных) целях.
- самостоятельно вносить какие-либо изменения в конфигурацию аппаратно-программных средств или устанавливать дополнительно любые программные и технические средства. При возникновении таковой необходимости следует обращаться в ОИТиС.
- использовать или подключать к ЛВС неучтенные технические средства, например съемные накопители («флешки»), телефоны, сетевые карты, модемы (GSM/Wi-Fi/WiMAX), фотоаппараты и т.п.
- приостанавливать, отключать или иным образом мешать штатной работе средств защиты.
- осуществлять поиск способов преодоления установленных мер защиты, а также использовать организационные, программные или технические средства, реализующие названные способы.
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или средствах защиты, которые могут привести к нарушению информационной безопасности.
- разглашать информацию, открывающую доступ третьих лиц к техническим средствам или данным, а также передавать кому-либо средства доступа к ним.
- осуществлять автоматическую переадресацию сообщений корпоративной почты в сеть Интернет.
- распространять программные продукты и иные материалы, не связанные со служебной деятельностью (нелицензионные программы, компьютерные игры, фильмы, музыку, художественную литературу, изображения и т.п.).
- оставлять включенным свое автоматизированное рабочее место (далее - АРМ) без личного присмотра, не активизировав средства защиты от несанкционированного доступа (например, временную блокировку экрана). Временная блокировка АРМ осуществляется путем одновременного нажатия комбинации клавиш «Ctrl+Alt+Del» с последующим нажатием кнопки «Блокировать компьютер», либо одновременным нажатием комбинации клавиш «⊞+L».

1. Пароль

Пароль является персональной секретной информацией. Каждый владелец пароля несет личную ответственность за его сохранность. При выборе пароля следует придерживаться следующих правил:

- длина не менее 6 символов;
- содержит заглавные и прописные латинские буквы, а также цифры и спец.символы (@#$%& и т.д.);
- никак не связан с владельцем (имена, памятные даты, номера документов, часть логина и т.д.);
- пароль нужно запомнить, чтобы не записывать на листочки и т.п.;
- выбирать разные пароли к разным системам.

ЗАПРЕЩАЕТСЯ:

- сообщать пароль кому бы то ни было;
- использовать пароль другого пользователя;
- использовать в работе пароль, если есть подозрение на его компрометацию;
- записывать пароли и оставлять их в общедоступных местах (в ящике стола, на мониторе, на обратной стороне клавиатуры, на отдельных листках бумаги и т.д.).

Если пароль был установлен не самостоятельно (выдан администратором) следует обязательно сменить его при первом входе в систему. При этом новый пароль должен отличаться от предыдущего не менее чем в 2-х позициях.

Для предотвращения попыток подбора пароля после 5 неуспешных попыток авторизации учетная запись пользователя автоматически блокируется. Для разблокировки пароля следует обращаться в ОИТиС. Если учетная запись была заблокирована БЕЗ вашего участия (что может говорить о попытке подбора пароля к вашей учетной записи), следует немедленно известить об этом ГКЗ.

2. Антивирусная защита

Для защиты от вирусного заражения в Обществе используется корпоративная антивирусная защита. Ответственность за соблюдение требований по антивирусной защите в рамках защиты своего АРМ возлагается на пользователя ЛВС, который в частности ОБЯЗАН:

- обеспечивать поддержание работоспособности средств антивирусной защиты на своем АРМ.
- знать основные способы проникновения вирусов, а также основные признаки проявления вирусной активности.
- подвергать обязательному антивирусному контролю (проверке) любую информацию в электронном виде (файлы и потоки данных любых форматов), получаемую и передаваемую, в том числе по телекоммуникационным каналам, а также информацию на локальных и съемных устройствах.
- в случае подозрения на вирусное заражение немедленно прекратить обработку информации и поставить в известность ОИТиС или ГКЗ, следовать их указаниям.

3. Доступ к информационным ресурсам

Получение доступа к информационным ресурсам (далее - ИР) ЛВС осуществляется на основании заявки, согласованной с руководителем структурного подразделения. В зависимости от вида ИР, форма заявки на предоставление доступа может отличаться. Более подробную информацию можно получить в ОИТиС или ГКЗ.

Доступ к ИР и действия с ИР протоколируются с целью выявления их несанкционированного использования, проведения проверок и расследования инцидентов. Каждый пользователь, получивший легитимный или несанкционированный доступ к ИР несет персональную ответственность за свои действия.

4. Коммерческая тайна

В Обществе установлен режим коммерческой тайны (далее - КТ), предусматривающий правовые, организационные и технические меры по охране конфиденциальности информации, которые включают определение перечня информации, составляющей КТ, ограничение доступа к информации, составляющей КТ, учет лиц, получивших доступ к информации, составляющей КТ, нанесение на материальные носители, содержащие информацию, составляющую КТ, грифа «Коммерческая тайна» и другие мероприятия.

До размещения информации, содержащей картографо-геодезические материалы, на персональных компьютерах работников и на информационных ресурсах Общества, необходимо согласовывать необходимые действия с ГКЗ путем представления электронной версии материалов на проверку.

5. Перечень документов для обязательного ознакомления

Основные нормативные документы по обеспечению информационной безопасности, с которыми работник должен быть ознакомлен и строго выполнять их требования расположены на общем ресурсе Общества в папке «Отдел ДОУ\Электронная библиотека\Группа по корпоративной защите\Для всех»:

- ✓ Политика информационной безопасности;
- ✓ Политика информационной безопасности локально-вычислительной сети;
- ✓ Политика информационной безопасности информационно-управляющей системы производственно-хозяйственной деятельности;
- ✓ Политика обработки персональных данных;
- ✓ Положение об обработке персональных данных;
- ✓ Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных;
- ✓ Положение о режиме коммерческой тайны;
- ✓ Инструкция по конфиденциальному делопроизводству;
- ✓ Перечень информации, составляющей коммерческую тайну, и иной конфиденциальной информации;
- ✓ Инструкция о порядке передачи информации, составляющей коммерческую тайну;
- ✓ Регламент работы с картографическими материалами;
- ✓ Регламент управления доступом пользователей;
- ✓ Регламент обеспечения ИБ при удаленном подключении к информационным системам и сервисам;
- ✓ Инструкция по организации антивирусной защиты в корпоративной информационной системе;
- ✓ Инструкция по обеспечению ИБ при управлении учетными записями пользователей;
- ✓ Инструкция по обеспечению ИБ при использовании сервисов корпоративной электронной почты и сети Интернет;
- ✓ Положение о порядке подготовки и предоставления информационных материалов СМИ;

6. Ответственность

За виновные действия, повлекшие порчу или уничтожение информации, несанкционированный доступ к информации, создание и использование вредоносных программ, нарушение правил работы с конфиденциальной информацией или внешними устройствами пользователи несут ответственность в соответствии с законодательством Российской Федерации, в том числе уголовным, трудовым договором или локальными актами Общества.

Мера административной или иной ответственности определяется по результатам расследования инцидентов.

Законом установлены следующие виды дисциплинарных взысканий: замечание, выговор, и в случае повторных нарушений, - увольнение по соответствующим основаниям.

При наличии в действиях работника состава преступления, предусмотренных статьями Уголовного кодекса Российской Федерации (УК РФ), Общество вправе обратиться с соответствующим заявлением в правоохранительные органы. В случае возбуждения уголовного дела по заявлению Общества, работник может быть привлечен к уголовной ответственности в порядке, установленном действующим законодательством РФ.

Статья 183 УК РФ. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок..

2. Незаконные разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, -

наказываются штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо исправительными работами на срок до двух лет, либо принудительными работами на срок до трех лет, либо лишением свободы на тот же срок.

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются штрафом в размере до одного миллиона пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями второй или третьей настоящей статьи, повлекшие тяжкие последствия, -

наказываются принудительными работами на срок до пяти лет либо лишением свободы на срок до семи лет.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

7. Контакты

По тел. 498214 (**Группа по корпоративной защите**) можно проконсультироваться по вопросам:

- содержимое документов из п.5;
- блокировка учетной записи заблокированной БЕЗ вашего участия;
- компрометация пароля;
- нештатная работа средств защиты (например, антивируса);
- утрата документов, содержащих конфиденциальную информацию;
- выявление факта разглашения информации ограниченного доступа (конфиденциальной информации).

По тел. 498232 (**ОИТиС**) следует обращаться по вопросам:

- неработоспособность технических средств или программ или обнаружение в них ошибок;
- вирусное заражение;
- разблокирование учетной записи заблокированной при вашем участии;
- сброс забытого пароля;
- заявки на доступ к информационным ресурсам.