УТВЕРЖДАЮ

Директор ФГБ ПОУ
«Кисловодский медицинский колледж»
Минздрава России
К.Н. Гоженко

«19» декабря 2023 г.

Политика информационной безопасности ФГБ ПОУ "Кисловодский медицинский колледж" Минздрава России

г. Кисловодск

2023 г.

Общие положения

Настоящая Политика информационной безопасности (далее Политика ИБ) содержит рекомендации и правила, направленные на снижение рисков нанесения финансового ущерба организации и её репутации, умышленного или по неосторожности (халатности) разглашения информации, несанкционированное распространение которой запрещено законами Российской Федерации (далее — РФ) и внутренними нормативными документами организации (далее — защищаемая информация). Работники организации несут ответственность за правонарушения с использованием систем автоматизированной обработки информации в соответствии с положениями статей 272, 273, 274 Уголовного кодекса РФ (Приложение 1).

Защита информации

Компьютеры пользователей, подключенные к сети Интернет, являются основным вектором атак злоумышленников на организацию. Для защиты информации организация использует стандартные в своей отрасли технические и организационные меры. Все корпоративные данные хранятся на контролируемых вычислительных ресурсах с ограниченным доступом.

Передача защищаемой информации деловым партнёрам и поставщикам организации оформляется надлежащими соглашениями о конфиденциальности NDA (Соглашение о конфиденциальности (NDA) между организациями (партнерами) регулирует взаимный обмен материалами, знаниями или другой информацией с ограничением доступа для третьих лиц).

Передача защищаемой информации через незащищенное соединение в сети Интернет осуществляется только при условии обеспечения защиты указанной информации от раскрытия и модификации. Работники организации принимают все доступные им меры для обеспечения гарантии безопасности и конфиденциальности защищаемой информации, за которую они несут ответственность, и которая им стала известна. В организации доступ к корпоративным ресурсам разрешён только для работников, прошедших установленную процедуру согласования доступа. Права предоставляются в соответствии со служебной необходимостью, определяемой руководством. Все полномочия по доступу являются персональными, указанными явно и проверенными ответственным лицом организации перед предоставлением доступа. По запросу на доступ к корпоративным ресурсам предоставляются полномочия минимально необходимые для реализации данного запроса. Принцип наименьших привилегий требует, чтобы в информационной системе, приложении или корпоративной сети пользователь имел возможность доступа только к той информации и ресурсам, которые необходимы для выполнения его служебных обязанностей.

Работа с общедоступными сетевыми ресурсами

При работе с ресурсами ЛВС пользователю запрещается:
– хранить информацию, составляющую служебную и коммерческую тайны на общедоступных сетевых ресурсах;
– пытаться увеличить объемы сетевых хранилищ и сетевых папок;
– передавать неустановленным порядком средства хранения информации третьим лицам;
– производить запись и хранить информацию не производственного характера;

– производить запись файлов, содержащих исполняемые коды или вредоносное программное обеспечение;
– копировать информацию и документы из ЛВС на незарегистрированные средства хранения информации;
– использовать незарегистрированные средства хранения информации для работы с информационными ресурсами и средствами ЛВС.

Организация удаленного защищенного доступа к ресурсам ЛВС и информационным системам

Удаленный доступ работников к сетевым ресурсам – сетевым дискам и директориям, расположенным в ЛВС организации, оформляет и предоставляет подразделение ИТ, в соответствии со служебной запиской руководителя структурного подразделения, согласованной с подразделениями безопасности.
Удаленный доступ к ЛВС, предоставляется для выполнения работ вне офиса, на период командировок или уход работника на удаленную работу на основании приказа. После возвращения работника из командировки или с удаленной работы, удаленный доступ отключается.
Удаленный доступ осуществляется при помощи дополнительно устанавливаемого программного обеспечения, создающего защищенное соединение с ЛВС – VPN соединение.
Пересмотр прав доступа производится в случае прекращения полномочий работника – переход на другую должность внутри организации и/или изменении требований руководящих документов по безопасности.

Защита от вредоносного ПО

В организации используются средства для защиты от вредоносного ПО (антивирусы). Однако, только антивирусной защиты в случае использования сети Интернет, недостаточно, так как существуют угрозы, которые могут не обнаруживаться антивирусами. Поэтому очень важно помнить о том, что нельзя открывать вложения в электронных письмах или переходить по ссылкам, полученным от неизвестных отправителей, а также загружать файлы с подозрительных сайтов в сети Интернет. С целью защиты от киберугроз, в организации применяются механизмы блокирования нежелательных веб-ресурсов.

Поведение в сети Интернет

Не посещайте сомнительные ресурсы в сети Интернет. Не размещайте в сети Интернет информацию, которая может навредить интересам компании, где вы работаете, и(или) вам лично. На всех платформах в сети Интернет, где у вас есть аккаунты и где позволяет соответствующий сервис, необходимо включать двухфакторную аутентификацию. Эта мера может помочь, если пароль для входа в аккаунт стал известен третьим лицам. Не сообщайте в социальных сетях персональный адрес корпоративной электронной почты в неслужебных целях. Не подписывайтесь на рассылку информации неслужебного характера на персональный адрес корпоративной электронной почты. Не обсуждайте в социальных

сетях подробности вашей работы. Используйте отдельную карту для покупок в сети Интернет и пополняйте эту карту денежной суммой, которую планируете потратить.

Пароли

Для получения доступа к корпоративной сети организации, к закрытым сервисам и программам требуется ввести имя пользователя (login) и пароль. Работник организации самостоятельно отвечает за сохранение в тайне сведений об его имени как пользователя и пароле. Пароли пользователя организации должны удовлетворять следующим условиям: -длина пароля должна составлять не менее восьми символов; -в пароле должны присутствовать большие и маленькие буквы латинского алфавита, цифры и спецсимволы; -время действия пароля должно составлять не более 90 дней; -пароли от разных систем и сервисов не должны повторяться. При подозрении на компрометацию своего пароля работник должен незамедлительно сообщить об этом своему руководителю.

Обновление программ

На рабочем компьютере настроено автоматическое обновление всех программ, включая операционную систему компьютера. Если обновления устанавливаются вручную, дистрибутивы скачиваются только с сайтов производителей. Программное обеспечение организации необходимо дополнять инструментами, которые будут отслеживать наличие уязвимостей и отсутствие обновлений в программах и операционных системах, поскольку злоумышленники нередко используют уязвимости, чтобы проникнуть на рабочие станции пользователей, а затем в корпоративную сеть организации.

Мобильные устройства*

Использование личных мобильных устройств в рабочих целях, несёт дополнительные риски, связанные с защитой информации. Не оставляйте мобильные устройства без присмотра в общественном месте и не передавайте их никому в пользование. Не создавайте на мобильных устройствах (корпоративных и личных) дополнительные (нелегитимные) сети (например: Wi-Fi) с целью передачи/получения информации.

*Под мобильными устройствами в данном контексте подразумеваются любые переносимые устройства: ноутбуки, смартфоны, планшеты и прочее.

Шифрование

Если на ваших устройствах хранится защищаемая информация, их следует шифровать, чтобы никто не смог ими воспользоваться в случае потери или кражи устройства. Для защиты электронных сообщений от доступа к ним посторонних лиц при передаче по незащищенным каналам связи применяется шифрование.

Электронная почта

Не открывайте электронные сообщения от незнакомых отравителей. Корпоративная электронная почта используется только для деловой переписки между работниками и контрагентами. Для организации совместной работы на основе электронной почты применяется программное обеспечение Microsoft Office Outlook.

Работа с носителями информации

Каждый работник несет персональную ответственность за использование носителей информации и обязан обеспечить их безопасное хранение. Категорически запрещается снимать несанкционированные копии с носителей с защищаемой информацией, знакомить с содержанием указанной информации лиц, не допущенных к работе с этой информацией, выносить оборудование, носители информации (в том числе бумажные) и программы за пределы организации без письменного разрешения руководства (в том числе для технического обслуживания, ремонта или утилизации). Всегда принудительно проверяйте с помощью средств антивирусной защиты съёмные носители информации после использования их вне офиса. Используйте только разрешенные к применению носители информации.

Защита данных на рабочих станциях пользователей и серверах

Объекты информационной инфраструктуры (в том числе, рабочие станции), прикладное программное обеспечение, технологии обработки защищаемой информации являются собственностью организации и могут быть использованы только в служебных целях. Покидая рабочее место, не забывайте блокировать компьютер нажатием комбинации клавиш CTRL-ALT-DEL. Не оставляйте гостей на территории организации без сопровождения. Не забывайте закрывать двери в помещение, в которую посторонним вход воспрещен. Измельчайте все бумажные документы, содержащие защищаемую информацию. Не забывайте распечатанные документы в принтере.

Хранение ЭЦП в организации

Место хранения электронного ключа должно быть защищено от чужого доступа. Требования законодательной базы предписывают:

1. Стороны электронного взаимодействия сохраняют конфиденциальность ЭЦП, обязуются защищать от использования без согласия владельца.
2. Владельцы уведомляют центр сертификации ключа о нарушении конфиденциальности ЭЦП, утрате или получении информации третьими лицами.
3. Запрещается использовать скомпрометированный ключ.
4. Применять методы проверки и соответствия электронного ключа.

Со стороны владельца подписи должна быть обеспечена защита данных. Если ключ не находится в хранилище, он должен быть установлен на каждый используемый ПК. Оговаривается круг лиц, имеющих доступ к документации и документообороту.

В законодательстве РФ описана ответственность за использование чужой ЭЦП. Не имеющие официального разрешения лица с доступом к чужому электронному ключу попадают под уголовную, административную и гражданско-правовую ответственность, оговоренную соответствующими кодексами.

В случае обнаружения нарушений уличенные лица несут уголовную ответственность электронная подпись считается скомпрометированной. Если действия личности причинили материальные убытки, ей вменяется возместить ущерб. Принимающая электронный ключ по договору личность несет полную ответственность за его хранение.

Приложение 1

Уголовный кодекс Российской Федерации
Глава 28
Преступления в сфере компьютерной информации

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.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.
2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

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.