Департамент информационных технологий и связи
Ямало-Ненецкого автономного округа

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ditis.yanao.ru ditis@yanao.ru +7 (34922) 2-20-22 Соцсети > «Информационные технологии и связь на Ямале»

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

Общие положения

Настоящие рекомендации разработаны в целях повышения уровня компьютерной грамотности сотрудников Законодательного собрания Ямало-Ненецкого автономного округа, исполнительных органов Ямало-Ненецкого автономного округа, иных органов государственной власти Ямало-Ненецкого автономного округа, органов местного самоуправления в Ямало-Ненецком автономном округе и подведомственных им учреждений и организаций (далее – сотрудник, государственный орган, автономный округ) и в рамках проведения профилактических мер по обеспечению информационной безопасности в государственных органах.

В результате изучения настоящих рекомендаций каждый сотрудник получит базовые знания по кибербезопасности, что позволит защитить себя и свои данные от киберугроз, снизит ущерб в результате кибератак и повысит общий уровень информационной безопасности государственных органов в целом.

Приведенные рекомендации по обеспечению информационной безопасности не носят исчерпывающий перечень мер, необходимый для обеспечения информационной безопасности в государственном органе. Каждый государственный орган должен самостоятельно определить и применять собственные, уточненные, меры по защите информации, учитывающие специфику своей информационной инфраструктуры и технологических бизнес-процессов обработки информации.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

ОБЩИЕ РЕКОМЕНДАЦИИ

- Обработка информации в информационных системах должна осуществляться только после активации средств защиты информации (Dallas Lock, ViPNet, антивирус Касперского и других). Убедитесь, что все средства защиты информации Вашего автоматизированного рабочего места работают.
- Не устанавливайте программное обеспечение самостоятельно, если это не входит в Ваши обязанности. Запуск программ, не относящихся к выполнению Ваших должностных обязанностей запрещен.
- Установка и использование нелицензионного программного обеспечения преследуется по закону. В архивах содержащих нелицензионное программное обеспечение, особенно если эти архивы получены из общедоступных источников, в большинстве случаев содержатся вредоносные программы.
- Не получайте доступ к автоматизированным рабочим станциям, если это не входит в исполняемые должностные обязанности.
- Не предоставляйте доступ к своему автоматизированному рабочему месту лицам, в случае, если такой доступ не предусмотрен их должностными обязанностями.
- Помните, использование программ для удаленного подключения к автоматизированному рабочему месту запрещено. В исключительных случаях, если обоснованна необходимость использования таких программ, допустимо использование программ, включенных в Единый реестр российских программ для электронных вычислительных машин и баз данных.
- Делайте резервные копии важных документов на защищенные носители (другой диск или внешний носитель, сетевой диск, облачное хранилище государственного органа и т.п.). Архивы, содержащие резервную копию, подлежат такой же защите, как исходная база данных и средства её обработки. Для настройки системы автоматического архивирования ценной информации и доступа к носителям архивных копий, обратитесь к ИТ-специалистам государственного органа.
- Располагайте мониторы и печатающие устройства таким образом, чтобы исключить несанкционированный просмотр отображаемой и распечатываемой информации. Не размещайте мониторы компьютеров вблизи окон, открытых дверных проемов и т.д.
- В случае выявления ошибки или деактивации средств защиты информации (Dallas Lock, ViPNet, антивирус Касперского и других), немедленно прекратите обработку информации и сообщите администратору информационной безопасности государственного органа.
- Не вскрывайте корпус системного блока, моноблока или ноутбука и не вносите изменения в состав технических средств. Ежедневно проверяйте, не нарушена ли целостность опечатывающей пломбы на используемом Вами устройстве.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

ПАРОЛЬНАЯ ЗАЩИТА

- Не используйте простые или распространенные пароли, например: "123456", "P@ssw0rd", "Qwerty321", "111111", "admin" и т.п. Пароли должны быть не менее 10 символов, содержать прописные и строчные буквы (a-z, A-Z), цифры и спецсимволы (&*!%).
- Меняйте пароли не реже чем один раз в 60 дней, при этом новый пароль должен отличаться от старого не менее, чем в 4 символах. Не используйте ранее введенные пароли.
- Сохраняйте в тайне личный пароль. Никогда и никому не сообщайте свой пароль, не храните записанный пароль на стикерах и не храните записанный пароль в общедоступных местах, в том числе на мониторе, клавиатуре и т.д.
- Если для производственных нужд пароль на время передавался другому сотруднику, то по завершению такой необходимости, незамедлительно самостоятельно смените этот пароль.
- Не используйте личные пароли (от соцсетей, личной почты и т.п.) для служебных информационных систем (рабочий компьютер, бухгалтерские и служебные программы, базы данных, и т.д.) и наоборот, не используйте служебные пароли для личных целей. В случае компрометации пароля для доступа к одной из используемых сервисов и информационных систем, тогда доступ будет утрачен к ним всем.
- Никогда не сохраняйте ваши пароли в программах или браузере, в том числе: для интернет - банков, личных кабинетов платежных систем и других сервисов с вашей или чужой персональной и служебной конфиденциальной информацией. Большинство программ хранят пароли в открытом виде и тот, кто получит доступ к вашему компьютеру, тот легко получит доступ и к вашим паролям!
- При кратковременном покидании рабочего места в течение рабочего дня в обязательном порядке блокируйте компьютер нажатием комбинации клавиш «Win + L» (в Microsoft Windows) либо «Ctrl + Alt + L» (в РЕД ОС). При долговременном покидании выключайте автоматизированную рабочую станцию.
- Если сервис или информационная система позволяет использовать двухфакторную аутентификацию, включите ее. Это не позволит злоумышленнику получить доступ к сервису даже в случае утечки пароля.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

АНТИВИРУСНАЯ ЗАЩИТА

- На компьютере, подключенном к локальной сети государственного органа или к информационно-телекоммуникационной сети «Интернет» (далее – Интернет) должен быть установлен антивирус.
- Если антивирус отсутствует, перестал обновляться или вовсе работать (на иконке антивируса появились восклицательные знаки, крестики или выдаются об этом сообщения на экране), то обязательно об этом сообщите администратору информационной безопасности Вашего государственного органа. Самостоятельно не отключайте антивирус!
- Обязательно проверяйте на наличие вирусов все съемные носители информации, которые подключаются к Вашему автоматизированному рабочему месту (CD, DVD-диски, USB-флеш-носители, карты памяти) и приложения к поступающим электронным письмам. Сделать это просто: правой кнопкой мыши на диске, папке или файле и выберите пункт "Проверить на вирусы" (называется по-разному в зависимости от установленного антивируса).
- Во всех случаях проявления действия вирусов или подозрении на наличие вируса не пытайтесь удалить вирус самостоятельно, незамедлительно сообщите об этом администратору информационной безопасности Вашего государственного органа.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

ИНТЕРНЕТ И ЭЛЕКТРОННАЯ ПОЧТА

- Всегда тщательно проверяйте с какого адреса отправлено письмо и куда ведут ссылки в письме (достаточно навести мышью на ссылку, не нажимая на неё). Убедительно выглядящее имя отправителя — не гарантия подлинности. Злоумышленники могут направить фишинговую ссылку, особенно если им удастся захватить почту кого-то из ваших коллег. Даже одна ошибочная буква в ссылке, якобы на официальный портал, может привести Вас на фишинговый портал.
- Рекомендуется проверять ссылки на незнакомые интернет-порталы, полученные от доверенного отправителя. Допустимо использовать официальный портал АО «Лаборатория Касперского» (https://opentip.kaspersky.com/) для проверки IP-адресов, файлов, доменов и веб-адресов. Портал оперативно определит и укажет на наличие реальной опасности. Ссылки на доверенные сервисы автономного округа (с окончанием «yanao.ru») отправке на проверку не подлежат.
- Не переходите по ссылкам, не запускайте программы и не открывайте файлы, полученные по электронной почте от неизвестного Вам отправителя или с подозрительным содержанием. В подавляющем большинстве случаев такие электронные письма содержат вредоносное программное обеспечение (вирусы). Например, таким вложением может быть вирус-шифровальщик, замаскированный под обычный служебный документ (.docx, .xlsx, .pdf и т.д.).
- Во всех случаях получения электронного письма от подозрительного источника или с подозрительным вложением, необходимо не предпринимать каких-либо действий в отношении данного письма и незамедлительно сообщить администратору информационной безопасности Вашего государственного органа.
- Не используйте Интернет для поиска или просмотра сайтов знакомств, игровых или развлекательных сайтов, содержащих суицидальные или порнографические материалы, содержащих материалы экстремистского или террористического характера, а также любые другие сайты, которые не относятся к направлению Вашей деятельности.
- Не используйте Интернет на рабочем месте для совершения личных коммерческих сделок, покупок, просмотра и распространения рекламы, коммерческих объявлений.
- Помните, использование социальных сетей (Одноклассники, Мой Мир, ВКонтакте и т.д.) и мессенджеров (Viber, WhatsApp, Skype, Discord, WeChat, Threema, Snapchat и т.д.) в личных целях на рабочем месте запрещено.
- Не передавайте электронные файлы содержащие служебную информацию ограниченного доступа и персональные данные по открытым каналам связи, особенно с использованием публичных облачных хранилищ данных (Яндекс Диск, Google Диск и т.д.), социальных сетей (Одноклассники, Мой Мир, ВКонтакте и т.д.) и мессенджеров (Viber, WhatsApp, Skype, Discord, WeChat, Threema, Snapchat и т.д.).

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

СЪЕМНЫЕ НОСИТЕЛИ ИНФОРМАЦИИ

- Подключение и копирование информации на учтенные съемные носители информации может осуществляться исключительно по согласованию или указанию Вашего непосредственного руководителя.
- Храните полученный съемный носитель информации (CD, DVD-диски, USB-флеш-носители, карты памяти) таким образом, который исключает несанкционированный доступ, утрату или кражу. Не оставляйте съемный носитель информации подключенным к автоматизированному рабочему месту и храните его таким образом, который исключит несанкционированный доступ.
- Все съемные носители информации подлежат хранению в сейфах или несгораемых шкафах, оборудованных замком.
- Не оставляйте съемный носитель информации в общедоступных местах, в автоматизированном рабочем месте и на столе.
- Съемные носители информации (CD, DVD-диски, USB-флеш-носители, карты памяти) не подлежат выносу из помещений государственного органа, в том числе для работы дома.
- Допускается передача информации в электронном виде на CD или DVD-диске, при наличии сопроводительного письма, подписанного руководителем государственного органа.
- Копирование служебной информации государственного органа на неучтенные или личные съемные носители информации запрещено!
- Хранение информации на съемных носителях должно осуществляться с использованием шифрования, это исключит несанкционированный доступ к ней, в случае утраты или кражи.
- Любое мобильное устройство (смартфон, планшет и т.д.) имеет память, которое при подключении воспринимается системой в качестве USB-флеш-накопителя. Поэтому подключение к автоматизированному рабочему месту мобильных устройств запрещено.
- Не подключайте к рабочему компьютеру неизвестно откуда взявшиеся флешки. Атака через зараженный внешний накопитель — это не фантастика: злоумышленники действительно могут подбросить устройство таким образом, что бы именно Вы нашли её.
- В случае длительного отсутствия на рабочем месте или при увольнении, обеспечьте передачу съемного носителя информации администратору информационной безопасности или непосредственному руководителю.
- Незамедлительно сообщайте администратору информационной безопасности обо всех фактах поломки, утраты, использовании в нарушение настоящих рекомендаций или нецелевом использовании съемных носителей информации (CD, DVD-диски, USB-флеш-носители, карты памяти).

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

При слове «кибербезопасность» все думают о том, как защититься от хакеров, использующих технические уязвимости информационных систем и сетей. Но есть и другой способ проникнуть в информационные системы и сети – через человеческие слабости.

Это и есть социальная инженерия: способ обманом заставить определенного сотрудника раскрыть информацию о технологии обработки информации или получить доступ к интересующей информации.

- Нужно помнить, технических мер по гарантированной защите от «социальной инженерии» не существует. Постоянно сохраняйте бдительность!
- Важно понимать, что существуют множество методик злоумышленника – «социального инженера». О наиболее часто используемых методиках и о сути «социальной инженерии» можно ознакомиться на официальном портале АО «Лаборатория Касперского» (https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks).
- Звонки от мошенников, представляющихся сотрудниками банков, это тоже метод социальной инженерии. Значительно участились звонки мошенников, представляющихся сотрудниками правоохранительных органов и органов прокуратуры, в котором применяется техника введения жертвы в стрессовое состояние. Внимательно ознакомьтесь с номером телефона, с которого Вам звонят, никогда не вступайте в разговор с такими лицами, положите трубку! Постоянно сохраняйте бдительность!
- Будьте в курсе новых угроз кибербезопасности – возьмите за привычку регулярно знакомиться с материалами, размещенными в доверенных источниках, таких как официальный сайт департамента информационных технологий и связи автономного округа (https://ditis.yanao.ru/activity/302/), официальная группа «Информационные технологии и связь на Ямале» (https://vk.com/ditisyanao) или Центр ресурсов АО «Лаборатория Касперского» (https://www.kaspersky.ru/resource-center). Своевременное получение знаний о новых методах атак, повышает шансы не стать жертвой от их реализации.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

ЭЛЕКТРОННАЯ ПОДПИСЬ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

- При работе с ключевыми носителями, содержащими электронную подпись (далее – ключевой носитель) важно соблюдать правила работы со средствами криптографической защиты информации, установленными в государственном органе.
- Сохраняйте в тайне сведения об обрабатываемой информации и о применяемых средствах криптографической защиты информации.
- Полученный ключевой носитель не подлежит копированию и передаче кому-либо. Допустимо использовать полученный ключевой носитель только на своём автоматизированном рабочем месте.
- Закрытая часть ключа электронной подписи не должна переноситься в реестр операционной системы.
- Храните полученный ключевой носитель таким образом, который исключает несанкционированный доступ, утрату или кражу. Не оставляйте ключевой носитель подключенным к автоматизированному рабочему месту.
- Ключевой носитель подлежит хранению в сейфе или несгораемом шкафу, оборудованном замком.
- Не оставляйте носитель электронной подписи в общедоступных местах, в том числе на своем рабочем столе, органайзере для канцелярии и т.д.
- Ключевой носитель не подлежит выносу из помещений государственного органа, в том числе для работы дома.
- Используйте только сертифицированные по требованиям безопасности информации ключевые носители российского производства.
- В случае длительного отсутствия на рабочем месте или при увольнении, обеспечьте возврат ключевого носителя администратору информационной безопасности.
- Незамедлительно сообщайте администратору информационной безопасности обо всех фактах компрометации, поломки, утраты или кражи ключевых носителей.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

СЛУЖЕБНЫЕ ДОКУМЕНТЫ ОГРАНИЧЕННОГО ДОСТУПА И ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- Работа со служебными документами ограниченного доступа и персональными данными (далее – служебные документы) должна осуществляться в соответствии с законодательством Российской Федерации и локальными правовыми актами государственного органа. Запрещена обработка служебных документов, если это не входит в Ваши должностные обязанности!
- Разместите свое рабочее место таким образом, которое исключает несанкционированный просмотр служебных документов посетителями, служебным персоналом, коллегами и иными лицами, у которых отсутствует право просмотра данных служебных документов.
- Все служебные документы подлежат хранению в сейфах или несгораемых шкафах, оборудованных замком. Указанные места хранения и служебный кабинет, в котором они расположены, должны закрываться на ключ по окончанию рабочего дня.
- Выходя из кабинета, убирайте служебные документы в места их постоянного хранения и не оставляйте на видном месте ключи от сейфа, несгораемого шкафа и кабинета.
- В случае длительного отсутствия на рабочем месте или при увольнении, обеспечьте передачу по акту приема-передачи служебных документов замещающему Вас сотруднику, либо непосредственному руководителю.
- Не уничтожайте и не выкидывайте в мусорную корзину служебные документы. Бракованные листы и черновики служебных документов подлежат уничтожению в бумагорезательных машинах (шредерах). Уничтожение служебных документов осуществляется исключительно специально назначенной комиссией и в порядке, установленным государственным органом.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

ЦИФРОВОЙ СЛЕД

Очень важно понимать, что любые действия, в том числе деструктивного характера, в сфере информационных технологий оставляют цифровые следы.

В случае проведения служебного расследования, по факту нарушения требований по защите информации в государственном органе и если деструктивные действия были совершены с использованием Вашего автоматизированного рабочего места, учетной записи или электронной подписи, цифровой след укажет на Вашу виновность.

Будьте внимательны при использовании информационных технологий и информационных систем государственного органа, выполняйте требования действующего законодательства Российской Федерации, нормативных правовых актов в сфере информационной безопасности и рекомендации представленные в настоящем документе, тогда в данном случае, риск быть виновником в инциденте информационной безопасности будет минимальный.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

На работе

РЕАГИРОВАНИЕ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

1. Возникновение компьютерного инцидента
2. Обнаружение компьютерного инцидента сотрудником
3. Передача информации администратору информационной безопасности
4. Проведение администратором информационной безопасности мероприятий, направленных на устранение компьютерного инцидента
5. Продолжение штатной эксплуатации информационной системы

Обо всех случаях обнаружения странного поведения автоматизированного рабочего места, получения подозрительных электронных писем, компрометации учетной записи, ключевого носителя, проявления вирусных заражений или о других событиях, касающихся обеспечения информационной безопасности государственного органа, следует незамедлительно сообщать администратору информационной безопасности.

Контакты администратора информационной безопасности следует хранить в удобном и доступном для Вас месте, позволяющем быстро связаться в случае экстренной ситуации.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

Вне работы

ПРИ РАБОТЕ ИЗ ДОМА

- Старайтесь не смешивать работу и личную жизнь. Разделяйте личные и корпоративные: учётные записи, пароли, устройства.
- Если вы вынуждены выполнять работу с домашнего компьютера, сперва позаботьтесь о его безопасности. Установите последние обновления операционной системы и прикладных программ.
- Используйте антивирусную программу и обновляйте базы сигнатур ежедневно. Рекомендуется использовать отечественное сертифицированное по требованиям безопасности информации средство антивирусной защиты.
- Для онлайн-покупок используйте виртуальную карту. Когда что-то хотите купить, просто переводите с основной карты деньги на нее и сразу же ими расплачивайтесь. Даже если злоумышленник похитит эти данные, Ваших денег он не получит.
- При регистрации на не доверенных сайтах и площадках для размещения объявлений, не используйте свои настоящие персональные данные. Например, очень часто мошенники пользуются сведениями, содержащими имя и номер телефона, которые указаны в базах данных Avito, Drom и т.д. Если Вам позвонили и обращаются по указанному Вами ненастоящему имени, Вы будете заранее знать, что разговариваете с мошенником.
- Используйте персональный файрвол.
- Не пользуйтесь торрентом и иными публичными файлообменниками. Не пользуйтесь пиратскими материалами. Избегайте недоверенные источники с потоковой трансляцией фильмов и музыки книг. Зачастую, на подобных ресурсах хранятся вредоносные программы.
- Не используйте чужие USB-флеш-накопители и другие внешние устройства, которые обладают постоянным запоминающим устройством.
- Шифруйте носители информации Вашего компьютера и мобильного устройства (смартфон, планшет и т.д.).
- Не пользуйтесь смартфоном с root-правами, а сетевыми устройствами или компьютером – в режиме администратора. Даже если хакер получит пароль к Вашей учетной записи пользователя, он не сможет изменить конфигурацию системы или что-либо в нее установить.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

Вне работы

ПРИ УДАЛЁННОЙ РАБОТЕ И В КОМАНДИРОВКАХ

- Бесплатный интернет – это как бесплатный сыр в мышеловке. По возможности не используйте его! Если это невозможно, то обязательно используйте VPN. Эта технология была создана, чтобы безопасно работать через небезопасный канал связи.
- Не обменивайтесь важной личной информацией в открытом виде. Используйте шифрование и устанавливайте пароли к архивам, в которых хранятся личные данные.
- Большинство утечек информации происходит в результате успешных атак хакеров на слабо защищенные сайты, сервисы, информационные системы или ресурсы, которые осуществляют сбор и хранение избыточных данных о посетителях. Узнавайте технологию обработки информации сайтом, сервисом, информационной системы или ресурсом, уточняйте, как происходит обмен данными, перечень обрабатываемых данных, места их хранения, как происходит идентификация и аутентификация, используются ли «cookie» файлы и другие значимые сведения. На основании полученной информации, внимательно оценивайте риски, связанные с использованием сайта, сервиса, информационной системы или ресурса, и принимайте взвешенное решение о необходимости их использования.

РЕКОМЕНДАЦИИ

ПРОФИЛАКТИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДИТиС ЯНАО

Полезные ссылки

Kaspersky Threat Intelligence Portal

https://opentip.kaspersky.com/

Социальная инженерия – защита и предотвращение

https://www.kaspersky.ru/resource-center/threats/how-to-avoid-social-engineering-attacks

ДИТиС ЯНАО. Информационная безопасность

https://ditis.yanao.ru/activity/302/

ВКонтакте. Информационные технологии и связь на Ямале

https://vk.com/ditisyanao

Советы по безопасности компьютера

https://www.kaspersky.ru/resource-center