Приложение №1
к приказу АО «Кронштадтский морской завод»
от 11.04.2025 № 190 05

Утверждена
Приказом Генерального директора
АО «Кронштадтский морской завод»
от 11.04.2025 № 190 02

ПРОГРАММА
проведения внепланового инструктажа с работниками завода о повышении бдительности при общении по телефону, сети Интернет, в том числе посредством мессенджеров (WhatsApp, Viber, Telegram и пр.), использовании в быту средств мобильной связи и телекоммуникации

Ведение

1.1. По фактам поджогов, подрывов, повреждений иными способами административных зданий, банкоматов, офисов организаций, объектов критической инфраструктуры, служебных автомашин государственных, в т.ч. правоохранительных органов, в отношении лиц, их совершивших, возбуждаются уголовные дела по статьям 167 («Умышленное уничтожение или повреждение имущества»), 205 («Террористический акт»), 281 («Диверсия») Уголовного кодекса Российской Федерации, предусматривающим в виде наказания длительные сроки лишения свободы, вплоть до пожизненного заключения, вне прямой зависимости от возраста, социального положения, состояния здоровья и степени осознания общественной опасности совершенного.

1.2. Проведение инструктажа по безопасности осуществляется с целью недопущения фактов уничтожения и повреждения имущества завода путем диверсий, а также утечки информации ограниченного доступа, о повышении бдительности при общении по телефону, сети Интернет, в том числе посредством мессенджеров, использовании в быту средств мобильной связи и телекоммуникации.

2. Администрация АО «Кронштадтский морской завод» информирует:

ВНИМАНИЕ МОШЕННИКИ!!!

Все виды мошенничеств условно подразделяются на контактные и бесконтактные. Контактные предполагают непосредственное личное общение злоумышленника со своей «жертвой». Бесконтактные мошенничества происходя с помощью телефонной связи либо сети-интернета, при этом «жертва» не видит преступника.

2.1. Бесконтактные мошенничества совершаются следующим способом:

*** Сотрудники банков и служба безопасности.**

Неизвестные лица в ходе телефонного разговора, представляются сотрудниками банков, сотрудниками службы безопасности, сотрудниками правоохранительных органов, сообщают о возможных мошеннических действиях со счетами, поступление денежных средств на счет от мошенников, оформлением кредитов, вводят «жертв» в заблуждение, после чего вынуждают переводить на счета мошенников собственные накопления, снимать денежные средства со своих счетов, оформлять кредиты, займы и также переводить на счета мошенников, как по номерам телефонов, так и на банковские карты. Переводы осуществляются под предлогом сохранения денежных средств пострадавших на, так называемых, «безопасных счетах».

*** Инвестиционная деятельность, биржа, крипто валюта.**

В сети интернет на различных платформах для знакомств (ВКонтакте, Одноклассники), в мессенджерах (Телеграмм), сеть-интернет (размещение сайтов, всплывающей рекламы, спамов) злоумышленники под предлогом осуществления инвестиционной деятельности, покупки крипто валюты, завладевают денежными средствами «жертв». По факту никакого отношения «жертва» к бирже и крипто валюте не имеет. Также злоумышленники используют различные мобильные приложения, где искусственно поднимают ставки и заработок «жертвы» с целью дальнейшего получения от последней денежных средств.

Сотрудники портала «Госуслуги», под предлогом предоставления различных справок и выписок, просят назвать код пришедший по СМС, после чего получают доступ к учетной записи и завладевают личными данными «жертвы»

Сотрудники операторов связи, под предлогом продления договора оказания услуг, просят назвать код из СМС, после чего получают доступ к порталу «Госуслуг». Далее к разговору могут подключиться сотрудники различных ведомств (Центробанк, полиция, безопасность банка и т.д.), которые сообщают «жертве», что с их счетами проходят мошеннические действия и для спасения денежных средств требуется выполнять их инструкции. После этого «жертва» отправляет на указанные неизвестным лицом счета, принадлежащие ему денежные средства.

Сотрудники правоохранительных органов под предлогом спасти деньги, накопления, просят изобличить преступников, выполнить важное задание для обеспечения безопасности страны, в том числе совершить поджог автомобиля, какого-либо объекта.

* **Сайты двойники (или фишинговые сайты).** Мошенники создают сайт двойник официального сайта, на котором совершаются онлайн-покупки. При этом «жертва» оплачивает услуги и переводит денежные средства на счет преступников. Через некоторое время сайт удаляется.

* **Авито, Юла доставка.** Под предлогом продажи (покупки) товара на сайтах злоумышленник предлагает оформить доставку, после чего отправляет ссылку. Перейдя по ссылке, «жертва» заполняет данные своей банковской карты, после чего происходит списание денежных средств.

* **Озон, Вайлдберрис.** Под предлогом продажи товара размещенного на странице продавца, «жертва» переводит денежные средства. Чаще всего товар не поступает, продавец перестает выходить на связь. Либо приходит товар не надлежащего качество, либо товар не соответствует заказанному.

Чаще всего в выше указанных ситуациях «жертва» ведется на товар, который продается ниже стоимости выставленный в магазинах или на официальных сайтах. В результате товар не предоставляется, денежные средства не возвращаются.

* **QR-коды** в парадных, лифтах, предлагающие вступить в группы в мессенджерах собственников жилья в жилищных комплексах, жителей улицы или благотворительных организаций - фишинг.

* **Сообщения в мессенджерах** типа «Привет, перейди по ссылки и проголосуй за моего родственника, который участвует в конкурсе» - фишинг.

СЛЕДУЕТ ПОМНИТЬ, ЧТО В НЕКОТОРЫХ СЛУЧАЯХ БЕСКОНТАКТНОЕ МОШЕННИЧЕСТВО ПРЕВРАЩАЕТСЯ В КОНТАКТНОЕ – когда дистанционный мошенник присылает к Вам за наличными деньгами курьера.

НЕЛЬЗЯ ПО ТЕЛЕФОНУ СООБЩАТЬ КОМУ-ЛИБО СВЕДЕНИЯ О СВОИХ СЧЕТАХ, ПАРОЛИ, КОДЫ ИЗ СМС. Не сообщать конфиденциальную информацию. Не следовать инструкциям мошенников. Прервать разговор. Позвонить в службу поддержки банка или по официальному номеру организации, от имени которой к вам обращаются. Перезвонить тому, о ком идет речь (в случае, если человек попал в беду)

Не реагируйте на сообщения с незнакомых номеров, в которых указаны ссылки для скачивания стороннего программного обеспечения или переход на какие-либо веб-страницы

ПРЕДСТАВИТЕЛИ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ, ЦЕНТРАЛЬНОГО БАНКА, АДМИНИСТРАЦИИ ГОРОДА, ГОСУСЛУГ ВАМ НЕ ПОЗВОНЯТ С ЦЕЛЬЮ СОХРАННОСТИ ДЕНЕЖНЫХ СРЕДСТВ ПУТЕМ ПЕРЕВОДА, И НЕ БУДУТ ПРОСИТЬ ИЛИ ТРЕБОВАТЬ ИСПОЛНЕНИЕ КАКИХ-ЛИБО ПОРУЧЕНИЙ.

С 01.03.2025 года граждане РФ могут установить самозапрет на выдачу кредитов. Можно установить запрет на заключение договоров потребительского займа с банками и микро финансовыми организациями.

2.2. Контактные мошенничества совершаются под различными предлогами, а именно:

* **Гадание и снятие порчи,** чаще всего совершается лицами «Цыганской внешности». На улице подходит женщина (мужчина), просит показать руку или по иным внешним признакам определяет наличие порчи на человеке. Под предлогом снятия порчи неизвестное лицо завладевает денежными средствами или золотыми украшениями, которые находятся на теле или дома у гражданина, после чего скрывается в неизвестном направлении.

* **Под различными предлогами** (социальные работники, аварийная служба, установка систем сигнализаций, газовых сигнализаторов, приборов тепло регулирования, получение надбавок к пенсии, замена старых денежных купюр в связи с деноминацией), проникают в квартиру, заговаривают «жертву» выясняют места хранения денежных средств и иных ценных предметов, после чего похищают их.

* **Обмен денежных средств или продажа монет царских времен.** Обмен денежных средств, как и продажа монет царских времен происходит на улице.

Цель, завладеть денежными средствами «жертвы». Денежные средства, которые передает злоумышленник являются купюрами «банка приколов». Царские монеты чаще всего приобретаются в сувенирных лавка или сети- интернет.

* **Продажа страховых полюсов.** Неизвестные лица осуществляют звонки на мобильные телефоны лицам у которых заканчивается или закончился срок страхования по страховому полюсу, после чего предлагает оформить новый. Согласившись, «жертва» фотографирует свои данные паспорта, водительское удостоверение, СТС и отправляет злоумышленникам. Через некоторое время курьер привозит готовую бланочную продукцию, «жертва» передает деньги курьеру. В результате проверки страхового полиса на официально сайте страхователя, бланк является недействительным.

* **Родственник попал в ДТП.** Чаще всего данному виду мошенничества подвержена незащищенная категория граждан (пенсионеры). Неизвестное лицо осуществляет звонки на мобильные или городские телефоны. Представляются сотрудниками полиции и сообщают, что по вине сына, дочери, внука, внучки произошло ДТП, в связи с чем потерпевший получил серьезные травмы. Да бы избежать уголовной ответственности, «жертве» необходимо дать взятку и решить вопрос обоюдно. Чтобы заверить в правдоподобности слов, разговор якобы переходит к родственнику, который просит «жертву» дать денег лицу, которое приедет по адресу проживания «жертвы». Через некоторое время приезжает неизвестное лицо, и жертва передает денежные средства наличным расчетом курьеру. Также возможны варианты с переводом денежных средств на счета самой «жертвой» через платежные терминалы.

2.3. Воздействие иностранных спецслужб может быть сложным и многогранным, реагирование на это требует комплексного подхода. Угрозы террористического и экстремистского характера представляют собой деструктивную идеологическую деятельность иностранных спецслужб, направленную на вовлечение российских граждан в противоправную деятельность, такую как:

– подготовка и совершение терактов и диверсий, прежде всего в отношении объектов транспортной и энергетической инфраструктуры, объектов Минобороны России, МВД России, Росгвардии, иных правоохранительных органов, административных зданий, объектов производства и военно-промышленного комплекса, финансово-кредитной сферы;

– передача информации о численности, вооружении, техническом оснащении, местах дислокации и передвижении подразделений Вооруженных Сил

Российской Федерации, расположении важных производств, генерирующих мощностей и др.

2.4. В качестве исполнителей преступлений на территории России террористические и экстремистские организации пытаются вербовать, в первую очередь, представителей молодежи из групп риска: оппозиционно настроенных, людей с наркотической зависимостью, граждан, находящихся в сложной жизненной ситуации.

2.5. У вербовщиков имеется определенный отработанный алгоритм действий:

– определение целевой аудитории, в том числе среди молодежи, людей, испытывающих материальные и социальные трудности, недовольных действующим государственным курсом, бунтарей и оппозиционеров, имеющих боевой опыт участия в военных конфликтах;

– сбор и анализ информации о потенциальной жертве для вовлечения ее в противоправную деятельность, прежде всего, посредством изучения профилей в социальных сетях;

– вступление в контакт с жертвой и «подсаживание на определенные крючки»: деньги и иные материальные стимулы, идеологические установки (например, радикально-оппозиционные), компрометирующие материалы, в том числе приватного характера, личные амбиции, желание отомстить.