НАЦИОНАЛЬНЫЙ РАСЧЕТНЫЙ ДЕПОЗИТАРИЙ
ГРУППА МОСКОВСКАЯ БИРЖА

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В НРД

Вводный инструктаж по информационной безопасности:

Угрозы ИБ и роль сотрудника
Противодействие фишингу и социальной инженерии
Работа в сети Интернет
Основы физической безопасности
Работа с носителями информации
Конфиденциальный документооборот
Реагирование на инциденты ИБ

Управление информационной безопасности
2018

Введение

Ответственным подразделением за процесс обеспечения информационной безопасности (далее - ИБ) в НРД является **Управление информационной безопасности.** Управление состоит из двух направлений:

- направление администрирование средств ИБ (каб. 5.30);
- направление защиты процессов и приложений (каб. 5.29).

Управление рисками ИБ осуществляется различными организационно-техническими мерами. При этом особый вклад в ИБ делают **Сотрудники**: разработчики, IT администраторы, пользователи.

Безопасность НРД, как и любой другой компании, сильно зависит от вклада каждого сотрудника.

Общие положения

- Пользователи НРД обязаны знать и выполнять требования внутренних нормативных документов НРД в части, касающейся информационной безопасности, своевременно проходить соответствующие курсы.
- При работе с информационными ресурсами НРД каждый Пользователь обязан не допускать утечки конфиденциальной информации.
- Ремонтные, профилактические работы и установку программного обеспечения производят только сотрудники ДСИТ.
- Каждый сотрудник имеет персональный логин/пароль для входа на компьютер. Не допускается его передача, в т.ч. технической поддержке, руководителю или сотруднику IT подразделений. При необходимости входа по Вашими учетными данными (например, в случае вашей болезни, отпуска) сбрасывается пароль при обращении в техническую поддержку sd@nsd.ru.

При первом входе на компьютер необходимо изменить первоначальный пароль.

Подключение к информационным ресурсам НРД

Доступ к информационным ресурсам предоставляется:

- в минимально необходимом объеме и может быть предоставлен и использоваться только в целях выполнения обязанностей работника, предусмотренных его должностной инструкцией, функционалом и не может использоваться в личных целях;

- на основании заявки на доступ к информационным ресурсам, которые инициируются через портал **ServiceDesk.nsd.ru.** руководителем работника (куратором) или коллегами. Изменение/добавление прав доступа работник имеет возможность запросить самостоятельно;

- после прохождения обучения (инструктажа) по соблюдению требованиям по ИБ при работе с информационными ресурсами (проводит УИБ).

Парольная политика НРД

Правила формирования паролей:

- пароли собственных учетных записей без привилегированных прав – всегда больше **10 знаков**.
- пароли учетных записей с наличием **привилегированных прав** – всегда больше **12 знаков**.
- **Должны содержать** как минимум **три группы** из четырех предложенных:
  - строчные латинские буквы: abcd…z
  - прописные латинские буквы: ABCD..Z
  - цифры: 0123456789
  - специальные символы: !@#$%^&*()_+ и аналогичные

При создании пароля более 16 знаков допускается брать любые две группы:

Пароли во всех случаях **не должны содержать**:

- словарных известных слов (вообще любых, в том числе русских слов, набранных на латинской раскладке)
- названий имен собственных, в том числе имен людей
- простых комбинаций, числовых, буквенных: 1111111, qwerty, asdf, password и аналогичных
- собственного имени, имен родственников, друзей, кличек животных
- названий почтовых ящиков, номеров телефонов, адресов
- дат и сочетаний дат в любых форматах (ГГГГММДД, ДДММГГГГ и т. п.)
- старых паролей от той же учетной записи – как минимум шесть последних значений
- паролей, которые уже используются в других системах

Работа с офисным и рабочим доменами НРД

В сети НРД организованы два основных домена:

- NSD – основной домен, где располагаются рабочие станции работников, осуществляется обмен почтовыми сообщениями, доступны сетевые хранилища, есть доступ в сеть Интернет и доступные офисные ресурсы, используемые для некритичных бизнес-процессов;

- NDCW – домен, где осуществляется ведение основных бизнес-процессов, отсутствует выход в сеть Интернет, прямой обмен файлами невозможен. Здесь применяются более строгие политики доступа.

Обмен информацией между доменами осуществляется с помощью специальных обменных директорий или с применением специально настроенных задач. Информацию об организации такого обмена можно получить в ДСИТ.

Работа с ресурсами НРД посредством личного оборудования

Работа с ресурсами НРД посредством личного оборудования допускается при условиях, когда со стороны руководства и УИБ было получено одобрение (через заявку).

- На личном оборудовании должно быть установлено антивирусное решение с постоянно обновляемыми базами (в случае, если для такого класса оборудования антивирусное ПО существует, например, для ноутбуков, персональных компьютеров, планшетов с ОС Windows и т.п.).
- Личное оборудование должно защищаться от несанкционированного доступа третьих лиц посредством:
  - пароля на вход (в соответствии с требованиями к паролям),
  - пин-кода длиной не менее 6 знаков (для мобильных устройств) и ноутбуков (шифрование).
- Удаленный доступ с личного оборудования к ресурсам НРД всегда должен через VPN доступ или опубликованные в сеть Интернет сервисы.
- Не допускается подключение личных ноутбуков напрямую к локальной сети НРД или добавление в домены.

Угрозы ИБ и роль пользователей

Чем же может помочь каждый сотрудник в обеспечении ИБ?

1. Придерживаться «**золотого правила**»: не делать ничего, что выходит за рамки должностных обязанностей.
2. Правильно реагировать на различные ситуации (в соответствии с Политиками ИБ), возникающие в ходе исполнения должностных обязанностей.

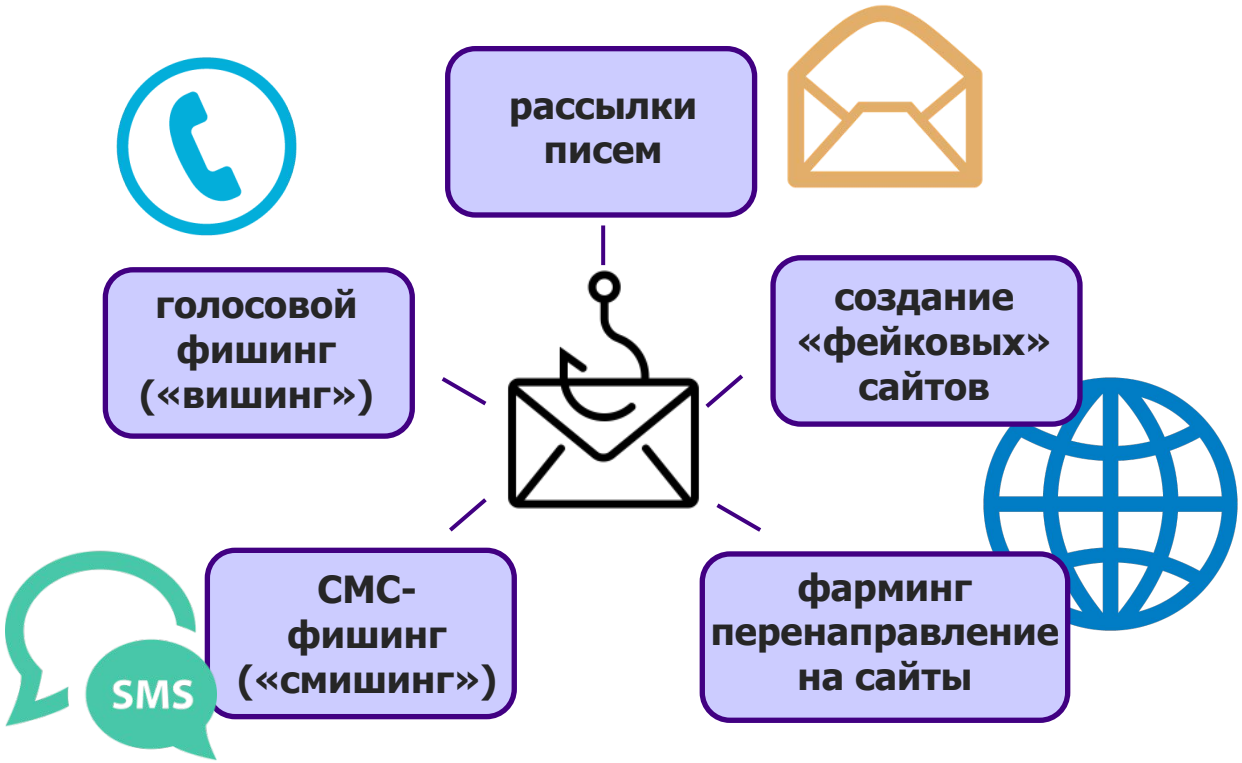
Рассмотрим актуальные на текущий день способы атак, в борьбе с которыми может помочь каждый сотрудник:

- фишинг;
- атаки с использованием сети Интернет;
- социальная инженерия;
- физическое подключение к сетям компании;
- использование вредоносного кода;
- манипуляции с носителями информации: кража, подбрасывание зараженных носителей и т.п.

Как правило, указанные способы комбинируются между собой. Например, чаще всего внутри фишинговых писем содержаться ссылки на фишинговые сайты или вложены вредоносные файлы, а текст письма составлен с применением техник социальной инженерии.

Фишинг

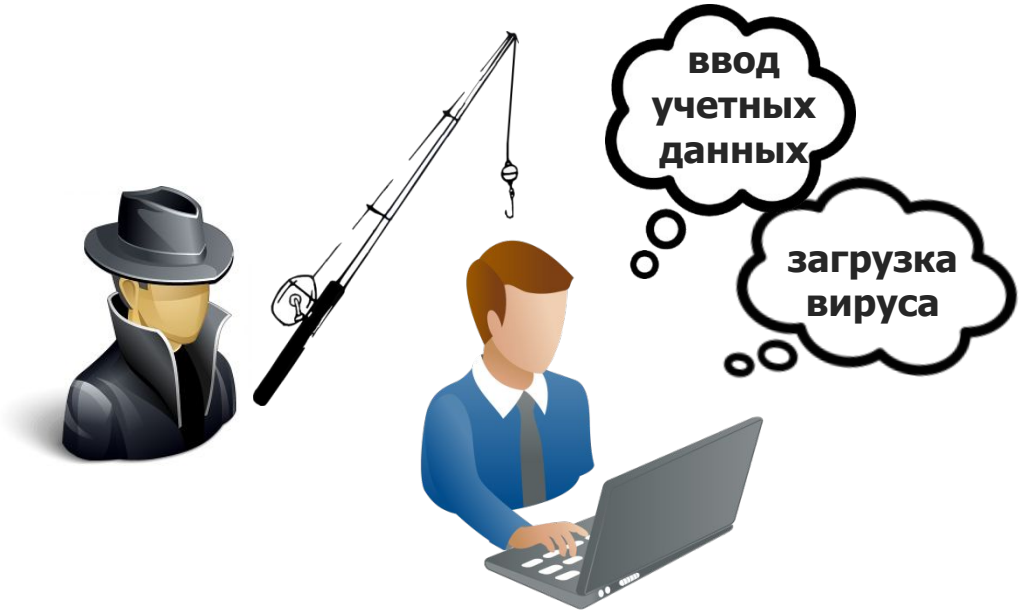
Q: Что такое фишинг?
А: Фишинг (от англ. Fishing – ловить рыбу) – вид **мошенничества**, для достижения целей которого злоумышленник **вводит пользователя в заблуждение.** Преследуемые цели:
– получение конфиденциальной информации;
– кража денежных средств;
– заражение компьютера.
В повседневной деятельности сотрудники, как правило, сталкиваются с фишинговыми рассылками и фишинговыми сайтами (похожими на настоящие, но таковыми не являющиеся).



Фишинговая рассылка

Цель мошенника: **заставить сотрудника ввести какие-либо данные на мошенническом сайте** (например, пароль от учетной записи) или попытаться **заразить компьютер вредоносным кодом** («трояны», «вирусы», «черви» и прочие представители Интернет-фауны), что может привести к:

- утечке конфиденциальной информации
- выполнению на рабочем компьютере любых злонамеренных действий, вплоть до удаленного управления компьютером.



Негативные последствия от фишинга:

- Сотрудники НРД тратят свое рабочее время на обработку совершенно ненужных сообщений от злоумышленников в ущерб основной деятельности;
- НРД тратит средства на покупку и внедрение защитных средств, позволяющих блокировать фишинговые и СПАМ-сообщения (множество не имеющих ценности сообщений);
- Применение средств защиты приводит к ложным срабатываниям и блокировкам действительно нужных сообщений, которые распознаются системой как фишинговые.

Фишинговые рассылки в НРД

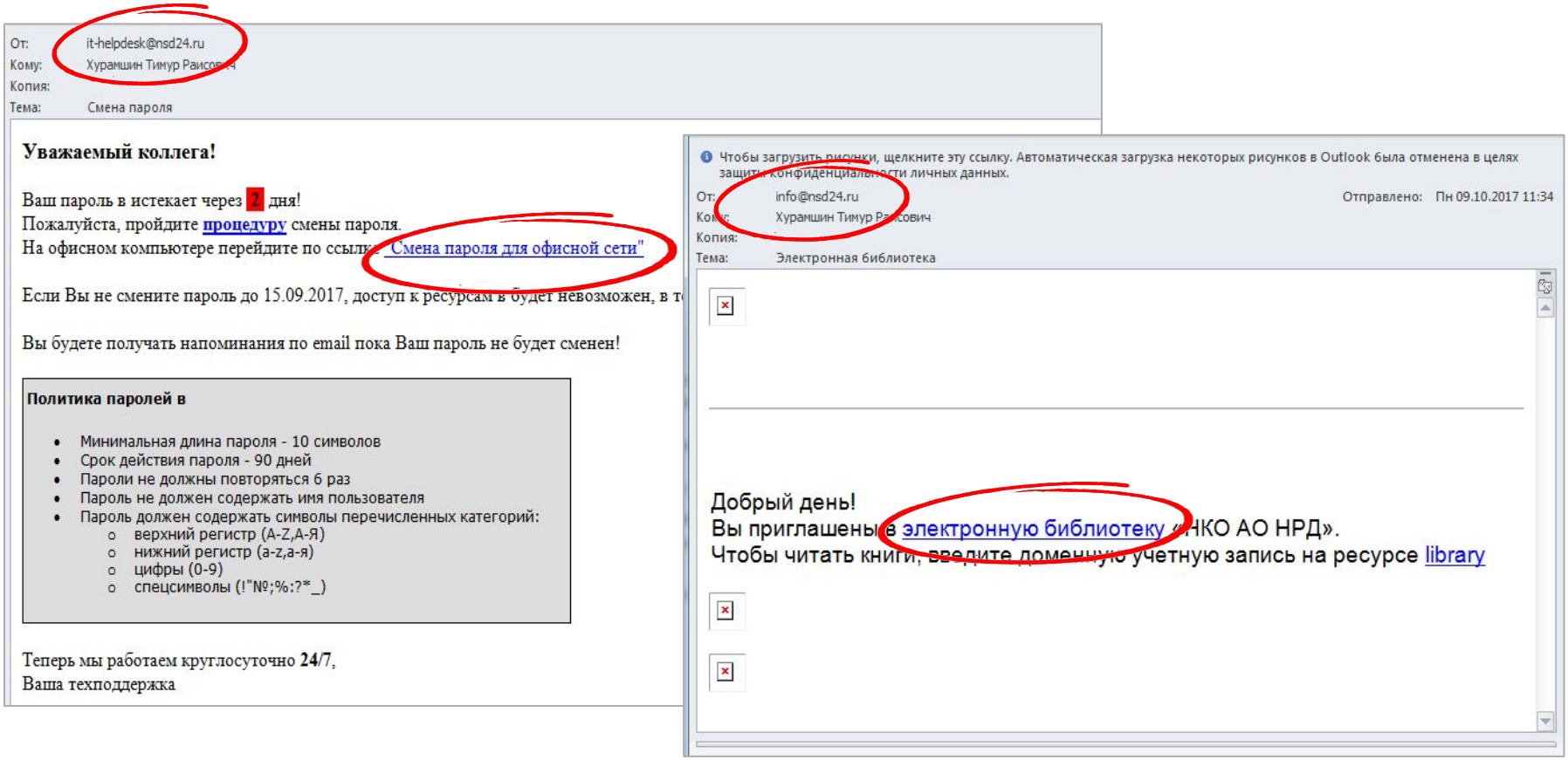
Управление ИБ проводит регулярные **проверки НРД на устойчивость к фишинговым атакам**.
На примере результатов проверки в октябре 2017 можно оценить **статистику реагирования сотрудников** на полученные ими различные письма, содержащие заманчивый текст (применение техник социальной инженерии) и ссылку на ресурс, который не принадлежал НРД.

Процент перешедших **по ссылке**.

Процент сотрудников, которые не только **перешли по ссылкам** из фишинговых писем, но еще и **ввели на поддельном (фишинговом) сайте данные**, которые запросил «злоумышленник».

Фишинговые рассылки в НРД

Примеры разосланных сообщений, которые получили сотрудники операционных и бизнес-подразделений:



От: it-helpdesk@nsd24.ru
Кому: Хурамшин Тимур Раисович
Копия:
Тема: Смена пароля

Уважаемый коллега!

Ваш пароль в истекает через 2 дня!
Пожалуйста, пройдите процедуру смены пароля.
На офисном компьютере перейдите по ссылке "Смена пароля для офисной сети"

Если Вы не смените пароль до 15.09.2017, доступ к ресурсам в будет невозможен, в т

Вы будете получать напоминания по email пока Ваш пароль не будет сменен!

Политика паролей в

- Минимальная длина пароля - 10 символов
- Срок действия пароля - 90 дней
- Пароли не должны повторяться 6 раз
- Пароль не должен содержать имя пользователя
- Пароль должен содержать символы перечисленных категорий:
  - верхний регистр (A-Z,А-Я)
  - нижний регистр (a-z,а-я)
  - цифры (0-9)
  - спецсимволы (!"№;%:?*_)

Теперь мы работаем круглосуточно **24/7**,
Ваша техподдержка

Чтобы загрузить рисунки, щелкните эту ссылку. Автоматическая загрузка некоторых рисунков в Outlook была отменена в целях защиты конфиденциальности личных данных.

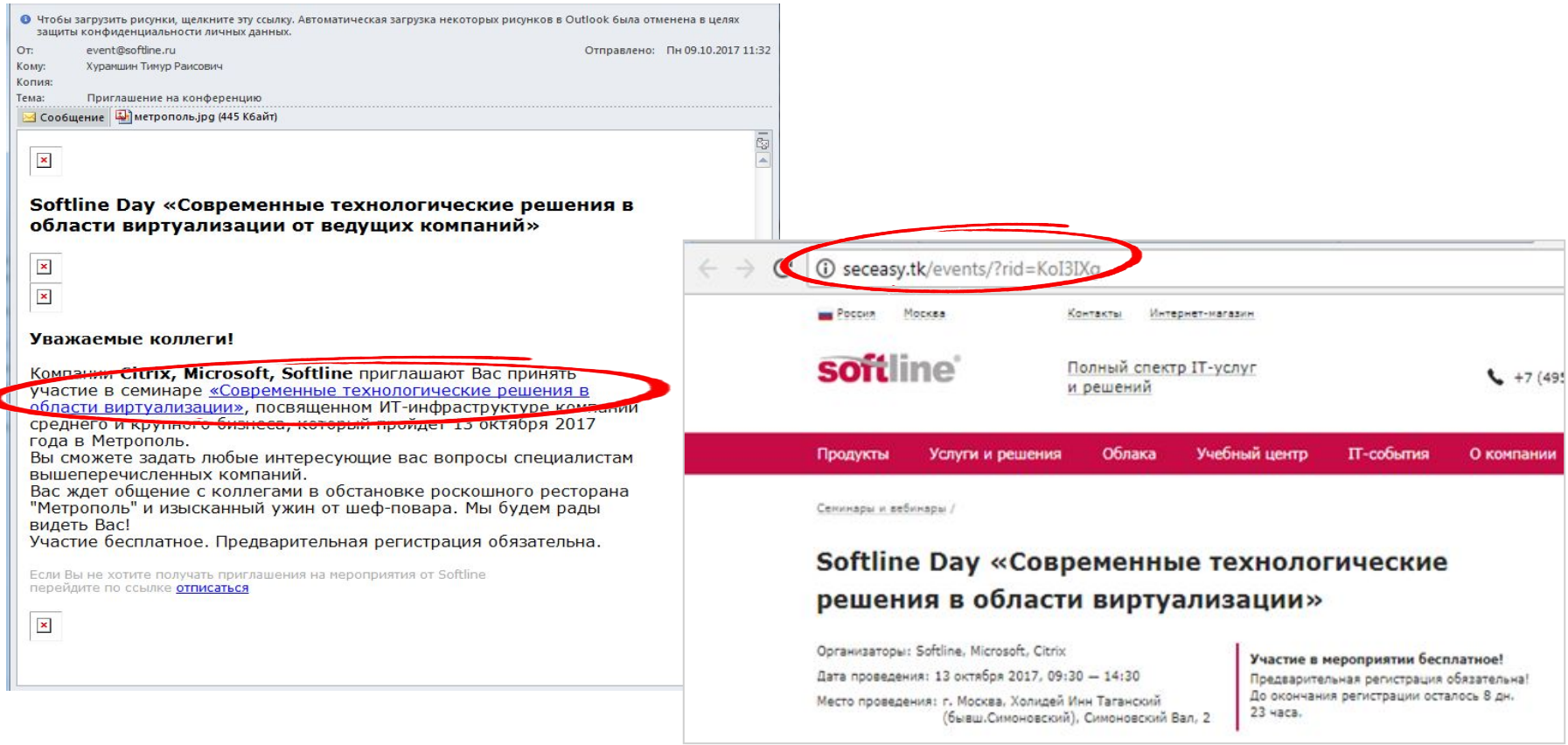
От: info@nsd24.ru
Кому: Хурамшин Тимур Раисович
Копия:
Тема: Электронная библиотека
Отправлено: Пн 09.10.2017 11:34

Добрый день!
Вы приглашены в электронную библиотеку «НКО АО НРД».
Чтобы читать книги, введите доменную учетную запись на ресурсе library

Обратите внимание, сообщение пришло с адреса **info@nsd24.ru**, в то время как все почтовые адреса НРД заканчиваются на **@nsd.ru** и не содержат ничего лишнего, в том числе «**24**».

Фишинговые рассылки в НРД

Примеры разосланных сообщений, которые получили сотрудники подразделений ИТ:



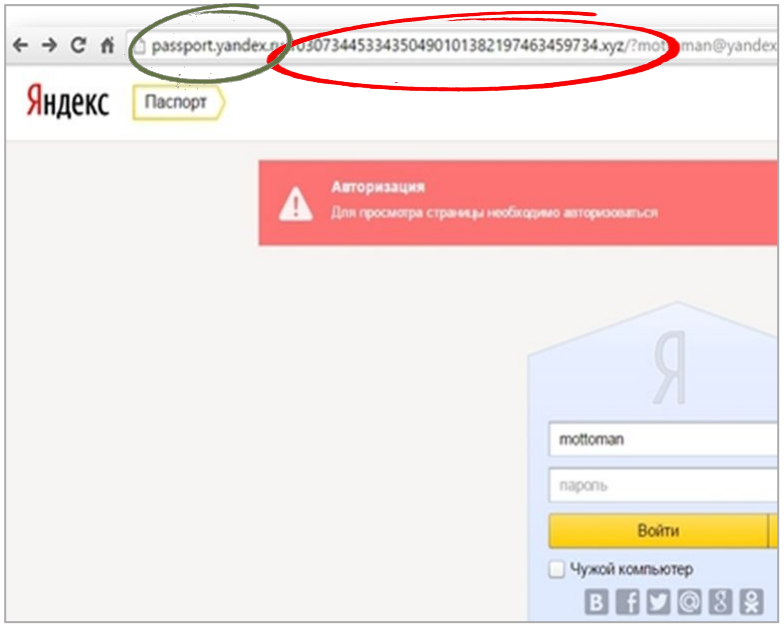
При открытии ссылок пользователя перенаправляет на сайт **seceasy.tk**, который не имеет никакого отношения к компании **Softline**. Хотя сайт и похож (визуально) на настоящий, но таковым не является.

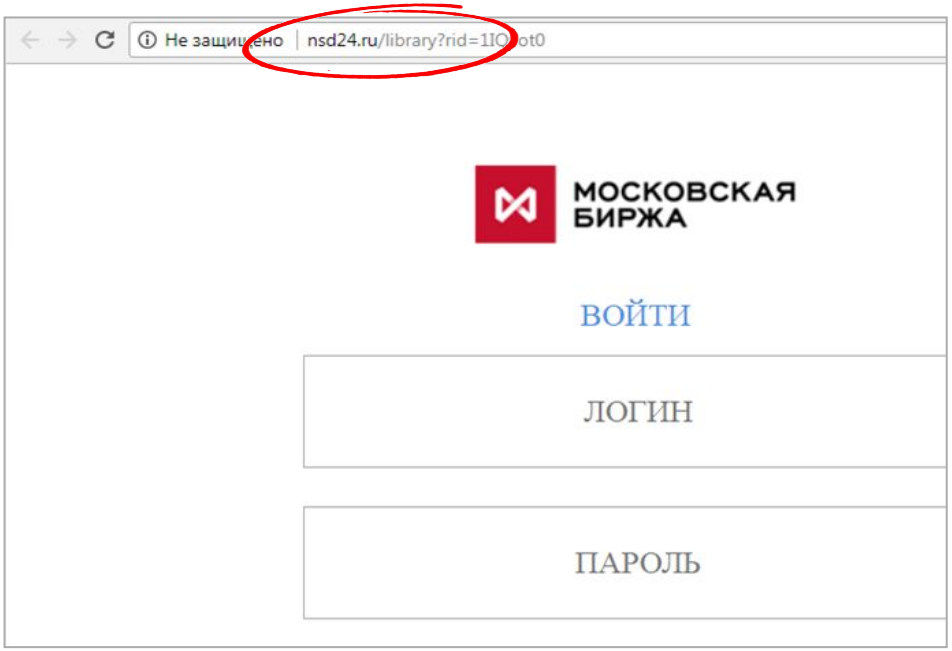
Фишинговые уловки - № 1 - тест на внимательность

Цель: Ввести жертву в заблуждение путем манипуляций с адресом отправителя.
Как выявить уловку: внимательно смотрим на **адрес отправителя** и ищем в нем неожиданные символы:

- Почтовая рассылка **от НРД** может прийти **только** от @**nsd.ru**. При этом после @nsd.ru не должно быть каких-либо дополнительных знаков и текста.
- Адреса @nsd.ru.fc, @nsd.ru.1212121.net, @nzd.ru, @insd.ru, @nsd.ru.com и им подобные не **принадлежат НРД.**

Такого рода уловки применяются и для **адресов сайтов**.
Ниже приведена настоящая фишинговая страница, направленная на атаку сервиса Yandex. **Обратите внимание**, что после «passport.yandex.ru» до знака «/» есть поле 1030734453343504901013821974634597 34.xyz. Этот набор цифр и есть **сайт злоумышленника**.
Также на втором скриншоте можно увидеть фишинговый сайт **nsd24.ru** из рассылки Управления ИБ, который маскируется под электронную библиотеку:





Фишинговые уловки - № 2 – тест на эмоциональную устойчивость

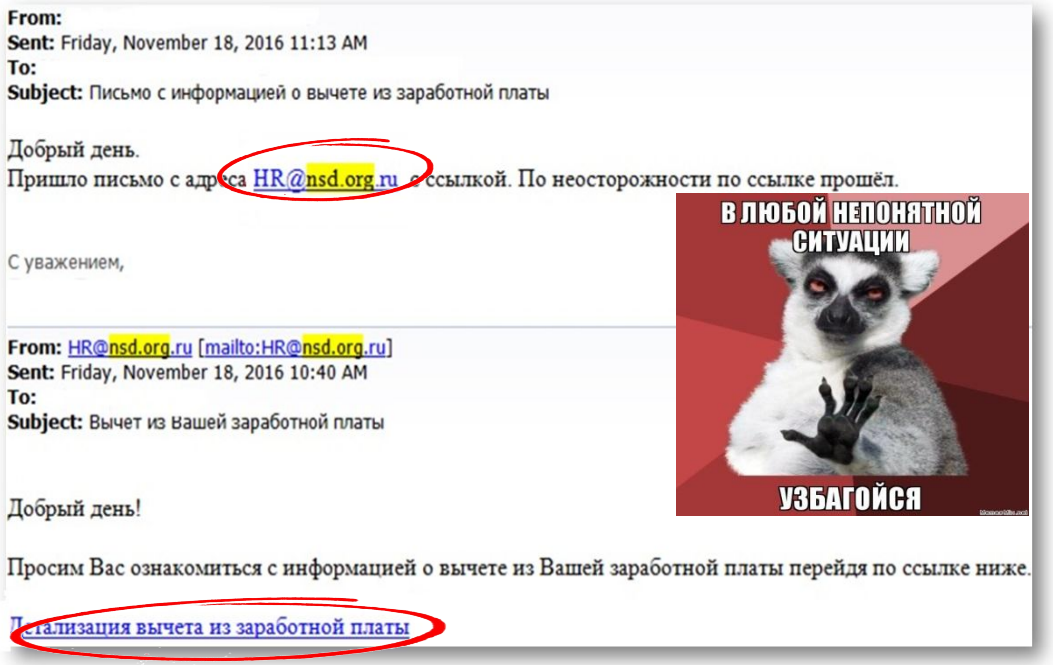
Цель: Создать стрессовую ситуацию, выполнить действие «здесь и сейчас»

Как выявить уловку: внимательно смотрим на **текст сообщения.** Вас должна насторожить любая попытка мотивировать на выполнение действия: просьба сменить пароль, нажать по ссылке, открыть файл во вложении, чтобы получить зарплатную ведомость и тому подобное мотивирование.

Письма злоумышленника составляются таким образом, чтобы побудить человека **немедленно и без раздумий выполнить требуемое действие**: как правило, кликнуть по ссылке в письме или открыть вложенный файл:

- «**СРОЧНО!!!!** Истекает пароль, требуется пройти по ссылке http://nsd.здесьмоглабытьвашареклама.net», иначе ваша учетная запись будет заблокирована в течение 5 минут.
- «Информируем Вас об изменении порядка получения зарплатных квитков. Более подробная информация по адресу: http://www.nsd.net.com».

Еще один пример письма, который отправлялся сотрудникам в 2016 году. Сообщение пришло с адреса hr@nsd.org.ru в то время, как адреса НРД не содержат лишних приставок «org», **текст письма** мотивирует его открыть как можно скорее – ведь речь идет о сокровенном - зарплате!



From:
Sent: Friday, November 18, 2016 11:13 AM
To:
Subject: Письмо с информацией о вычете из заработной платы

Добрый день.
Пришло письмо с адреса HR@nsd.org.ru с ссылкой. По неосторожности по ссылке прошёл.

С уважением,

From: HR@nsd.org.ru [mailto:HR@nsd.org.ru]
Sent: Friday, November 18, 2016 10:40 AM
To:
Subject: Вычет из Вашей заработной платы

Добрый день!

Просим Вас ознакомиться с информацией о вычете из Вашей заработной платы перейдя по ссылке ниже.

Детализация вычета из заработной платы

Пример реального фишингового сообщения

На общий ящик НРД Committee@nsd.ru пришло письмо с вложением в запароленном архиве. Внутри архива файл Документы на подпись.scr. Что не так с письмом:

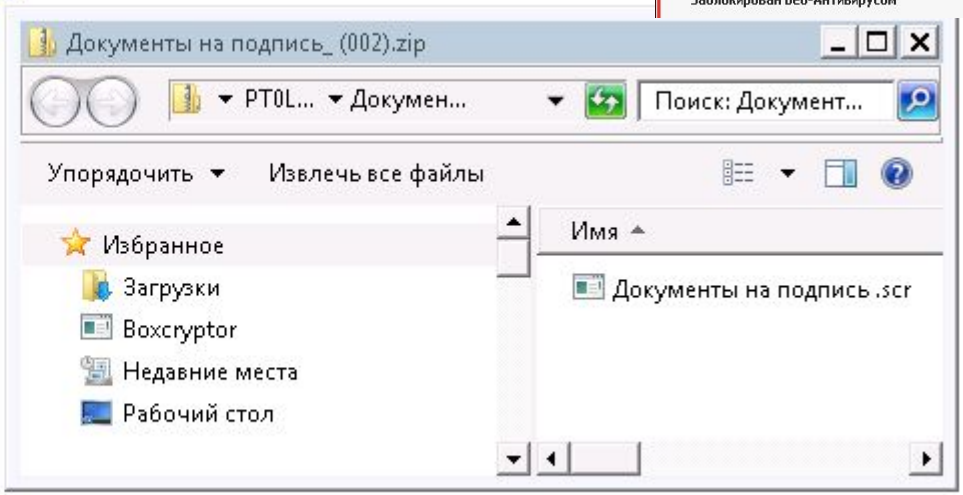
- Адрес поддельный, хоть и похож на настоящий (фишинговый сайт http://mastercard-europe.com/);
- У НРД нет Процессинга банковских карт и Мастер кард не является нашим клиентом;
- Срочность. «Вернуть сканы до конца дня»;
- Странное вложение с расширением scr. На самом деле это исполняемый файл, являющийся вирусом;
- Запароленный архив, который необходим злоумышленнику, чтобы обойти защиту.

From: Mastercard Europe [mailto:security@mastercard-europe.com]
Sent: Friday, February 10, 2017 2:18 PM
To: Committee
Subject: Бумаги на подпись

Добрый день,прошу подписать и вернуть сканы до конца дня.

Пароль: mastercard

Elena Prorokova
PR Director, Communications
elena_prorokova@mastercard-europe.com
tel +7 495 937 77 10



Пример реального фишингового сообщения

На общий ящик сотрудника НРД пришло письмо со ссылками от имени @online.vtb24.ru. В конце vtb24.ru и такой домен действительно существует и он принадлежит ВТБ24.

Что не так с письмом:

- Сотрудник никогда не контактировал с этим человеком из ВТБ24;
- Текст письма вызывает подозрение. Ранее ВТБ24 не выставлял счета;
- В письме есть ссылки и они не имеют отношения к ВТБ24, хотя визуально кажется, что все нормально. Достаточно подвести курсор и увидеть, что ссылка на самом деле такая: hovedprosjektblog.hig.no. Не всегда есть возможность подвести курсор. В этих случаях можно скопировать адрес ссылки, но не переходить по ней. Адрес ссылки вставить в документ или смс при использовании смартфона. Это позволит увидеть настоящий адрес.

Если открыть такую ссылку, компьютер может заразиться вирусом.

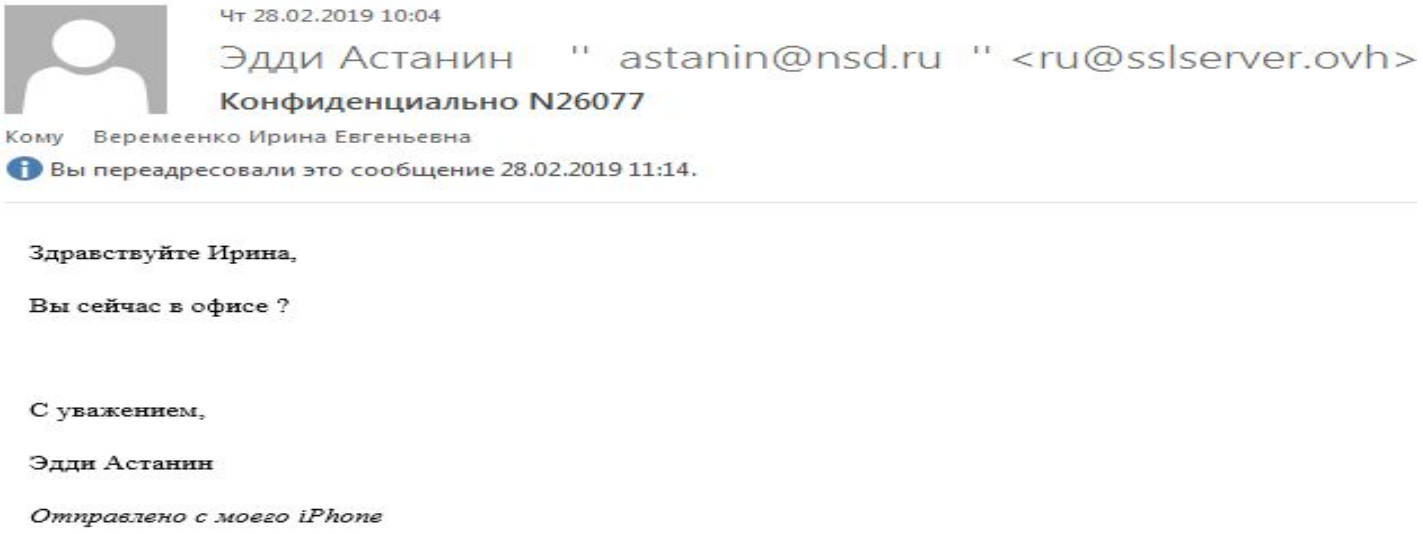
Пример реального фишингового сообщения

На почтовый ящик главного бухгалтера пришло письмо от имени «Астанина Эдди Владимировича»

Что не так с письмом:

- Обратите внимание на строку отправителя «Эдди Астанин «astanin@nsd.ru» <ru@sslserver.ovh>». Настоящий отправитель не заключается в кавычки. В данном случае письмо отправлено с ящика ru@sslserver.ovh.

Если увидели малейшую странность в письме. Особенно если вас побуждают совершить действия, которые в конечном счете могут привести к потере конфиденциальной информации, переводу денежных средств, СВЯЖИТЕСЬ с Вашим руководителем. Не стесняйтесь! Если руководитель недоступен, обратитесь в Управление информационной безопасности. Обращаю внимание, что почтовый ящик Вашего руководителя может быть даже взломан. И письма будут идти от его имени. Будьте бдительны!



Чт 28.02.2019 10:04

Эдди Астанин '' astanin@nsd.ru '' <ru@sslserver.ovh>

Конфиденциально N26077

Кому Веремеенко Ирина Евгеньевна

Вы переадресовали это сообщение 28.02.2019 11:14.

Здравствуйте Ирина,

Вы сейчас в офисе ?

С уважением,

Эдди Астанин

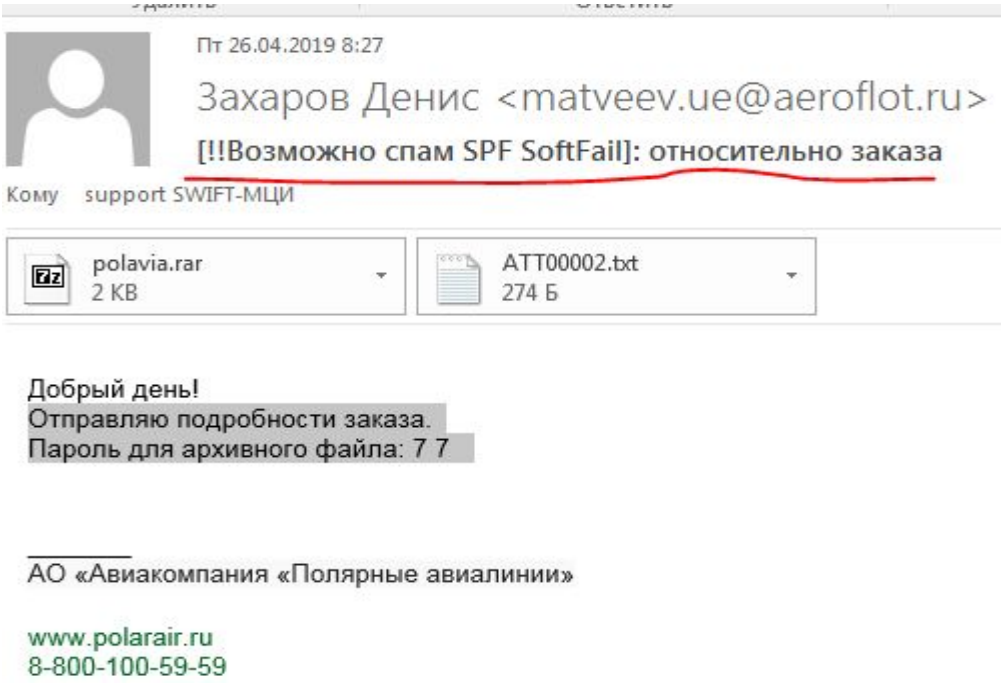
Отправлено с моего iPhone

Пример реального фишингового сообщения

На почтовый ящик поддержки пришло письмо из Аэрофлота. Причем адрес отправителя вроде бы корректен.

Что не так с письмом:

- Обратите внимание на тему письма [!!Возможно спам SPF SoftFail]. Такую пометку ставит система защиты НРД в тех случаях, когда адрес отправителя плохо защищает свой домен. В данном случае это Aeroflot.ru. От имени данной компании любой желающий может направить письмо. Это еще не означает, что письмо поддельное. В этом случае нужно обратиться в Управление информационной безопасности.



Пт 26.04.2019 8:27

Захаров Денис <matveev.ue@aeroflot.ru>

[!!Возможно спам SPF SoftFail]: относительно заказа

Кому support SWIFT-МЦИ

polavia.rar
2 KB

ATT00002.txt
274 Б

Добрый день!
Отправляю подробности заказа.
Пароль для архивного файла: 7 7

АО «Авиакомпания «Полярные авиалинии»

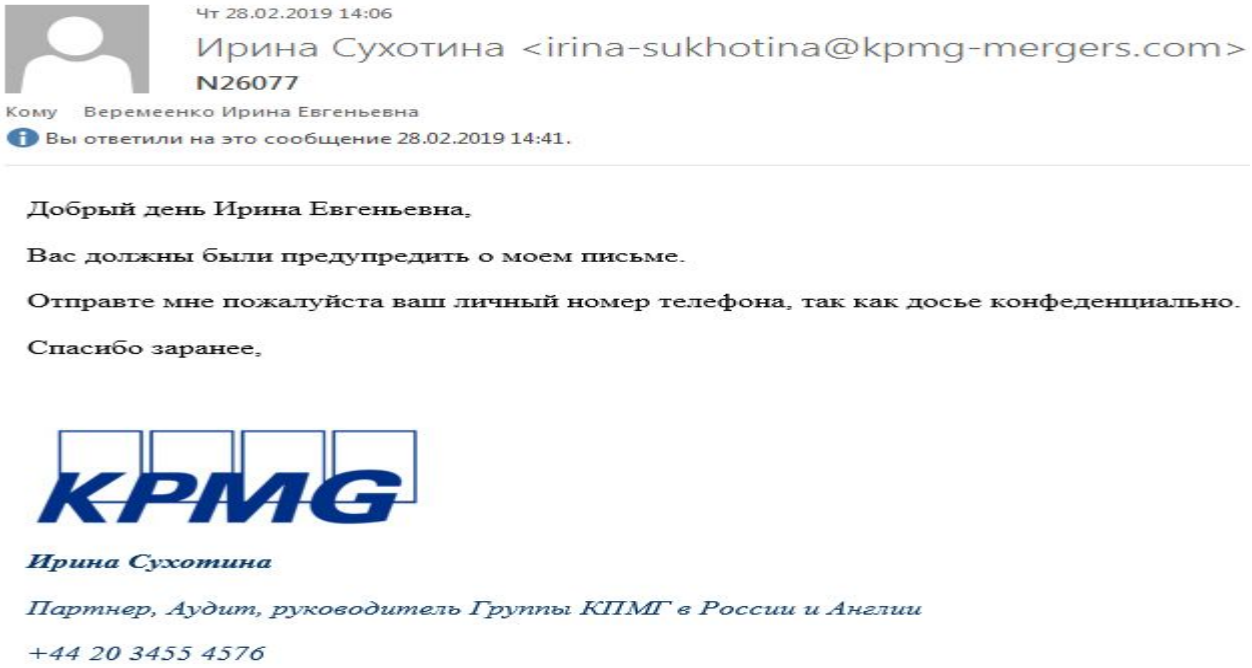
www.polarair.ru
8-800-100-59-59

Пример реального фишингового сообщения

На почтовый ящик сотрудника пришло письмо якобы от имени kpmg. Интересно то, что в KPMG действительно работает сотрудник Ирина Сухотина. Но связаться с ней не удалось. А при открытии домена kpmg-mergers.com открывается НАСТОЯЩИЙ сайт KPMG https://home.kpmg

Что не так с письмом:

- Домен kpmg-mergers.com не принадлежит KPMG. Как находить официальные сайты компаний? Можно просто вводить в google запрос вида «официальный сайт компании KPMG». Если найденный сайт не совпадает с отправителем, значит, вас пытаются обмануть. Более продвинутый способ: зайти на сайт who.is. Ввести адрес проверяемого домена и проверить поле org.
- Также стоит отметить, что настоящий сайт KPMG **https://home.kpmg** открывался при обращении на kpmg-mergers.com ввиду настроенного (специально!) перенаправления.



Чт 28.02.2019 14:06

Ирина Сухотина <irina-sukhotina@kpmg-mergers.com>

N26077

Кому Веремеенко Ирина Евгеньевна

Вы ответили на это сообщение 28.02.2019 14:41.

Добрый день Ирина Евгеньевна,

Вас должны были предупредить о моем письме.

Отправте мне пожалуйста ваш личный номер телефона, так как досье конфеденциально.

Спасибо заранее,

KPMG

Ирина Сухотина

Партнер, Аудит, руководитель Группы КПМГ в России и Англии

+44 20 3455 4576

Как распознать фишинг?

Фишинговые сообщения могут прийти с **любых** адресов. Например, были случаи заражения вирусом компьютеров регулятора и рассылки фишинговых писем в банки. Не бывает доверенных адресатов. Помните об этом!

Тем не менее есть несколько признаков фишинговых сообщений:

- незнакомый адрес отправителя письма или адрес, немного отличающийся от настоящего
- необоснованная срочность и мотивация на определённые действия
- наличие подозрительных ссылок в теле письма
- наличие вложенных файлов
- непонятный текста письма, причем текст письма может не коррелировать с вложениями, ссылками

Если вы столкнулись с **фишингом:**

- не открывайте ссылки/вложения в письме и
- сообщите об инциденте в Управление информационной безопасности, своему непосредственному руководителю, прикрепив полученное письмо с темой «Подозрительное письмо».

Если у вас возникли сомнения относительно полученного письма/ визита на сайт и даже если вы успели открыть письмо или открыть ссылку – немедленно обращайтесь в Управление ИБ.

Мы оперативно проанализируем ваше обращение и дадим обратную связь.

Социальная инженерия

Социальная инженерия (СИ) - способ получения информации и реализации других угроз, основанный на использовании особенностей психологии людей. **Человек всегда является слабым звеном** любой системы - поэтому **атаковать его проще**. **Очень часто социальная инженерия комбинируется с другими техниками**.

Примеры социальной инженерии:

- злоумышленник представляется другим человеком: родственником, попавшим в беду, сотрудником технической поддержки, который пытается вам помочь;
- шантаж, вымогательство;
- попытка сподвигнуть человека на действия, искусственно создавая стрессовые ситуации: «Вам пришел штраф, срочно пройдите по ссылке и оплатите», «ваш друг попал в беду, необходимо перечислить деньги», «ваш пароль истекает через 1 день, продлите его, пройдя ссылке, иначе вы не сможете работать», «вам начислены пени за неуплату счета».

Сотрудники Группы обладают информацией и знаниями, которые могут заинтересовать третьих лиц. В этих условиях очень важно выработать **критическое мышление** при взаимодействии с другими людьми.

Примеры атак с использованием СИ

Целевая атака на сотрудника организации

1. Злоумышленник **присылает письмо с фишинговой ссылкой** на почтовый адрес НРД определенному сотруднику (например, в кадровую службу, контакты которой можно найти на сайте НРД).
2. После чего злоумышленник **звонит** сотруднику по телефону, представляется, сообщает о письме и просит его открыть. Несмотря на то, что файл выглядит подозрительно, злоумышленник может придумать убедительную легенду, чтобы заставить HR специалиста открыть файл. Например, резюме прислано в зашифрованном архиве, мотивируется это тем, что человек боится разглашения своих данных. «Соискатель» при этом говорит пароль, чтобы Вы могли открыть архив. На самом деле, зашифрованный архив нужен для того, чтобы обойти системы защиты НРД, проверяющие вложенные в письма файлы.
3. И сотрудник, открывая такое письмо, подвергает риску всю компанию.

«Посмотрите, пожалуйста, я направлял письмо, но оно могло попасть в карантин, моя почта вам ведь незнакома, могла не пройти через фильтр. Посмотрите еще в нежелательных, могло и туда упасть, это нормально, пароль от архвива ЗДЕСЬМОГЛАБЫТЬВАШАРЕКЛАМА»

«Хорошо…»

Примеры атак с использованием СИ

Персональное воздействие, общение тет-а-тет

Очень часто, злоумышленники **представляются сотрудниками технической поддержки**. Обратите внимание, кто Вам звонит! При возникновении подозрений, попросите представиться сотрудника и перезвоните ему, посмотрев его номер на портале.

«Чтобы решить проблему нужно зайти с вашими учетными данными в систему, но я сейчас не могу к вам подойти и не знаю когда смогу, тем более это займет порядка нескольких часов и вы все это время будете без компьютера, а удаленно без ваших учетных данных проблему не решить..»

"Ой, да ну ладно, не первый день знакомы, вот мой логин/пароль, сообщи тогда, когда закончишь, ок?.."

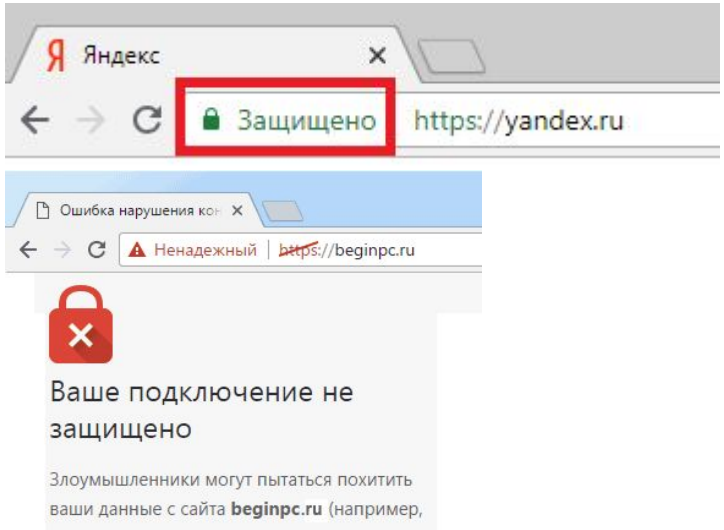
Интернет в НРД

Интернет через офисные компьютеры организуется только для выполнения сотрудниками должностных обязанностей.
Сеть интернет содержит множество угроз. Например,
- поддельные сайты;
- вредоносные элементы, встроенные в различные объекты на сайтах.

Иногда простой вход на сайт может привести к взлому компьютера.

Основные принципы работы в сети Интернет:

- **Сеть Интернет используется только для выполнения должностных обязанностей.**
- Для **личных целей** используем сеть **Wi-Fi** и личные устройства доступа: планшеты, мобильные устройства.
- При использовании внешних информационных ресурсов (электронных сообщений, гиперссылок, интернет сайтов и т.д.) Пользователь должен осознавать опасность возникновения угроз информационной безопасности НРД при использовании данных ресурсов не по служебной необходимости. Пользователь по возможности не должен использовать не вызывающие доверия информационные ресурсы.
- Если слева от адреса ресурса в адресной строке в Интернет-браузере значок замка и он зеленого цвета, то Ваше соединение с данным ресурсом защищено.
- Если слева от адреса ресурса в адресной строке в Интернет-браузере Предупреждение о ненадежности ресурса, то ресурс, на который Вы Пытаетесь зайти является ненадежным.
- При работе в сети Интернет, Пользователь должен убедится, что имя сайта совпадает с его настоящим именем (например, что буква «О» не заменена на «0» - ноль). Безопасно использовать ссылки из папки «Избранные» или вбивать адрес сайта вручную.



НРД автоматически протоколирует все действия пользователей сети Интернет, журналы посещений сайтов анализируются.

Работа с носителями данных и ключами СКЗИ

Не используем носители информации в личных целях

Всегда отключаем носители от рабочих станций, когда не используем их активно. Не оставляем подключенными без присмотра. К **ПИН-кодам** от токенов относимся так же ответственно, как к личным паролям. ПИН-код, установленный по умолчанию, меняем.

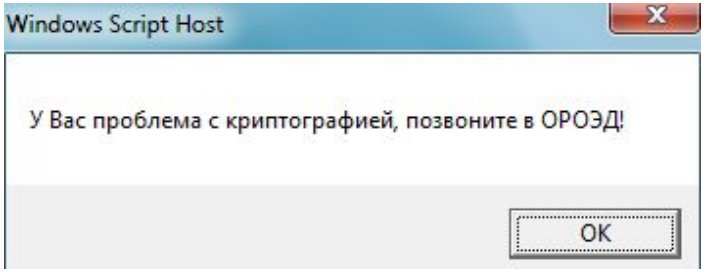
При подключении носителя к рабочей станции - убеждаемся, что **проверка антивирусом произведена**. Используем носитель только после нее (при этом вирусы должны были либо не найдены, либо успешно удалены. При любом неуспехе - относим носитель в Управление ИБ).

СКЗИ, токены, дискеты - храним в сейфах всегда, когда не используем активно. В персональных сейфах храним без ограничений, в сейфах с общим доступом - в опечатанных личной печатью пеналах.

Не копируем и не уносим на носителях конфиденциальные сведения без разрешения Управления ИБ и непосредственного руководителя.

Утеря носителя или обнаружение чужого - повод обратиться в Управление ИБ незамедлительно. Не подключаем носители информации к компьютерам с целью установления владельца носителя.

При появлении сообщения о проблеме с криптографией, обязательно оформить заявку на sd@nsd.ru для устранения ошибки. Работа с системами, использующими крипторгафию при наличии данного сообщения запрещается!



Правила физической защиты

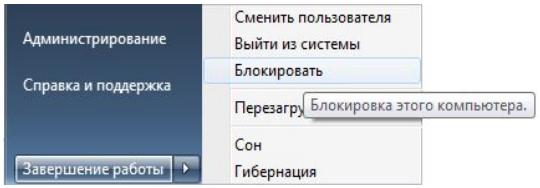
- **Соблюдаем установленный контрольно-пропускной режим, не пускаем в офис посторонних, не идентифицированных лиц.**
- **Не передаем никому свой пропуск.**
- **При утере пропуска** - немедленно **сообщаем** в Управление безопасности, не ждем окончания отпуска или выходных. Пусть лучше пропуск потом найдется, чем по нему успеет пройти злоумышленник.
- **Не пытаемся подключать к рабочим станциям флешки или диски, найденные в офисе или на пороге офиса.** Несем такие флешки в Управление ИБ.
- **Не ведем разговоры и переговоры, предполагающие озвучивание конфиденциальных данных, на улице и в присутствии посторонних.**
- В НРД организованы **специальные переговорные комнаты, куда можно водить посетителей без оформления пропусков** (1.5, 1.6, 1.7, 1.8, 1.9). Не смотря на то, что в переговорных организована отдельная инфраструктура (ноутбук, монитор), часть из оборудования которой "пристегнуто" к составным элементам здания, необходимо стараться не оставлять посетителей без присмотра. **При обнаружении подозрительных лиц** в данных переговорных следует **оповестить Управление безопасности**. Для доступа во все остальные помещения НРД реализуется пропускной режим - необходимо заказывать пропуска в УБ и сопровождать посетителей всегда.

Правила чистых столов и экранов

Не оставляем без присмотра конфиденциальные документы на рабочих поверхностях (на принтере, на рабочем столе и т.п.). **Убираем в запираемый шкаф, ключи носим с собой. Не «прячем» пароли под клавиатуру!**

При необходимости уничтожения бумажных документов используем **шредер**

При необходимости оставить рабочее место блокируем рабочий стол путем нажатия на клавиатуре сочетаний **«Win+L»** или **«CTRL+ALT+DELETE»,** выбираем опцию **«Блокировать компьютер».** Альтернативный, но долгий путь: меню **«Пуск» – «Блокировать»**



Нельзя передавать коллегам и кому бы то ни было свои именные учетные записи, а также пользоваться чужими.

Распечатки с принтеров, если только он не стоит один в кабинете, **забираем незамедлительно**, пока их не забрал кто-то другой.

Нашли чужие распечатки на принтере? Отнесите в Управление ИБ. Пусть даже эти распечатки попали в руки к вам вместо владельца, но мы будем уверены, что на этом они свое "путешествие" прекратят.

Конфиденциальная информация

Перечень конфиденциальной информации НРД:

Банковская тайна	Сведения об операциях, о счетах и вкладах клиентов и корреспондентов (а также иные сведения, устанавливаемые НРД). Информация по конкретным операциям. Не может быть передана третьим лицам.	Федеральный закон "О банках и банковской деятельности"
Тайна клиринговых операций	Информация, предоставляемая клиринговым организациям и лицам, осуществляющим функции центрального контрагента.; об обязательствах, в отношении которых проводится клиринг, сведения, предоставляемые участниками клиринга, информация о торговых счетах депо и торговых товарных счетах, об операциях по указанным счетам, о которой стало известно в связи с оказанием клиринговых услуг и (или) осуществлением функций центрального контрагента. Может быть передана третьим лицам, подписавшим NDA.	Федеральный закон 7.07.2010 N 224-ФЗ
Тайна депозитарных операций	Информация о счетах и об операциях клиентов центрального депозитария. Лицевой счет (счет депо), а также информации о таком счете (в т.ч. о держателе), включая операции по нему. Может быть передана третьим лицам, подписавшим NDA.	Федеральный закон N 414-ФЗ "О центральном депозитарии"
Тайна репозитарного обслуживания	Информация, получаемая Репозитарием НРД на основании договоров об оказании репозитарных услуг, а также информация, составляющая реестр договоров Репозитария, полученная в связи с осуществлением функций трансфер-агента, полученная держателями реестра и депозитариями. Не может быть передана третьим лицам.	Федеральный закон 22.04.1996 N 39-ФЗ "О рынке ценных бумаг"

Конфиденциальная информация

Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В том числе ФИО, номер телефона, адрес, почтовый адрес, дата рождения, дата смерти и т.п. Может быть передана третьим лицам, подписавшим NDA и при наличии согласия субъекта персональных данных (и в случаях отсутствия необходимости согласия)	Федеральный закон "О персональных данных" ФЗ-152
Инсайдерская информация	Существенная, публично не раскрытая служебная информация компании, которая в случае её раскрытия способна повлиять на рыночную стоимость ценных бумаг компании - согласно перечню инсайдерской информации НРД. Может быть передана третьим лицам, подписавшим NDA и при наличии лица в списке инсайдров.	Федеральный закон 7.07.2010 N 224-ФЗ
Коммерческая тайна	Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. Сведения, указанные в Перечне конфиденциальной информации НРД. Может быть передана третьим лицам, подписавшим NDA.	Федеральный закон N 98-ФЗ "О коммерческой тайне"
Для внутреннего использования (ограниченного использования)	Информация, являющаяся конфиденциальной с точки зрения НРД, не отнесенная ни к одной из выше перечисленных категорий информации, и к которой могут устанавливаться отдельные требования по защите и обеспечению конфиденциальности, например, информацию можно использовать внутри НРД кому угодно либо отдельным подразделениям, но которая не подлежит распространению вовне НРД. Сведения, указанные в Перечне конфиденциальной информации НРД. Может быть передана третьим лицам, подписавшим NDA	Внутренние требования организации

Конфиденциальный документооборот

- Электронные письма без применения криптографии считаются открытым каналом передачи данных, поэтому при необходимости отправки конфиденциального документа по электронной почте внешнему адресату, необходимо использовать запароленный архив. Пароль от архива сообщается по другим каналам связи. Например, по телефону.
- При использовании СВЭД Дело пользуйтесь грифами секретности, не направляйте документы неограниченному кругу лиц.
- При отсутствии понимания, является ли канал передачи данных безопасным необходимо обратиться в Управление ИБ.
- Не выносим за пределы компании конфиденциальные документы без разрешения непосредственного руководителя и Управления ИБ. Ограничения касаются как бумажных, так и электронных носителей информации.
- При необходимости уничтожения бумажных документов используем шредер, при необходимости уничтожения электронных носителей обращаемся в Управление ИБ или Отдел системного администрирования.

Реагирование на инциденты

Инцидент - событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.
Примеры инцидентов:

- получение сотрудником фишингового сообщения;
- попытки социальной инженерии;
- заражение компьютера вредоносным кодом: неожиданные всплывающие окна, аварийное завершение программ (особенно антивируса), неожиданно появляющийся черный экран (при этом это не мерцание экрана), появление на компьютере или сетевых дисках файлов с длинными или нечитаемыми именами, захват управления мышкой и клавиатурой неизвестными лицами;
- попытки «купить» у Вас информацию;
- пзвестные Вам случаи нарушения Политик ИБ или подозрения о таких нарушениях;
- попытки узнать Ваши персонифицированные логины/пароли.

В случае возникновения подобных ситуаций необходимо обратиться в Управление информационной безопасности и известить непосредственного руководителя.

Работа с электронной почтой

- перед отправкой сообщения по электронной почте необходимо проверять список получателей, текст сообщения и вложенные файлы;
- запрещено использовать корпоративную почту в личных целях, равно как и для отправки личных сообщений;
- запрещено использовать любые (в том числе бесплатные публичные) почтовые сервисы для отправки корпоративной информации;
- запрещено общаться с клиентами и партнерами, используя личные e-mail адреса;
- запрещено отправлять конфиденциальную информацию по электронной почте на внешние адреса в незащищенном виде;
- запрещено открывать письма от недостоверных источников, с подозрительными ссылками и вложениями;
- запрещено использовать корпоративный электронный ящик для подписок на сайтах, не связанных с выполнением должностных обязанностей;
- запрещено включать автоматическую переадресацию входящих сообщений на любые внешние адреса.

Обязанности работника

- выполнять требования Инструкции по обеспечению парольной защиты, правила и требования Положения по обеспечению ИБ при управлении доступом, парольной защиты;
- своевременно формировать и подавать данные карточки учета в УИБ для неперсонифицированной/разделяемой учетной записи;
- осуществлять немедленную смену скомпрометированных паролей и иных аутентификационных факторов;

- перед началом работы проверять целостность пломбировочной наклейки на системном блоке своего ПК;
- сохранять в тайне пароли доступа к информационным системам, в том числе обеспечивать сохранность паролей разделяемых учетных записей и контролировать допуск к ним посторонних лиц;
- своевременно информировать УИБ об обнаруженных инцидентах ИБ и случаях нарушений установленных процедур и правил.

Выполнение роли Куратора

Работник с назначенной ролью Куратора работника сторонней организации или практиканта (далее – РСО) дополнительно должен выполнять необходимые функции:

- Быть осведомленным об актуально составе РСО в своем подчинении, их фактической занятости.
- Своевременно подавать информацию о занятости РСО на работе в НРД, в том числе при необходимости изъять или изменить полномочия по доступу (не позднее 1 рабочего дня по факту возникновения обстоятельств, требующих внесения изменений в доступ РСО).
- Контролировать прохождение РСО учебных курсов по вопросам ИБ, выделять на это необходимое время.

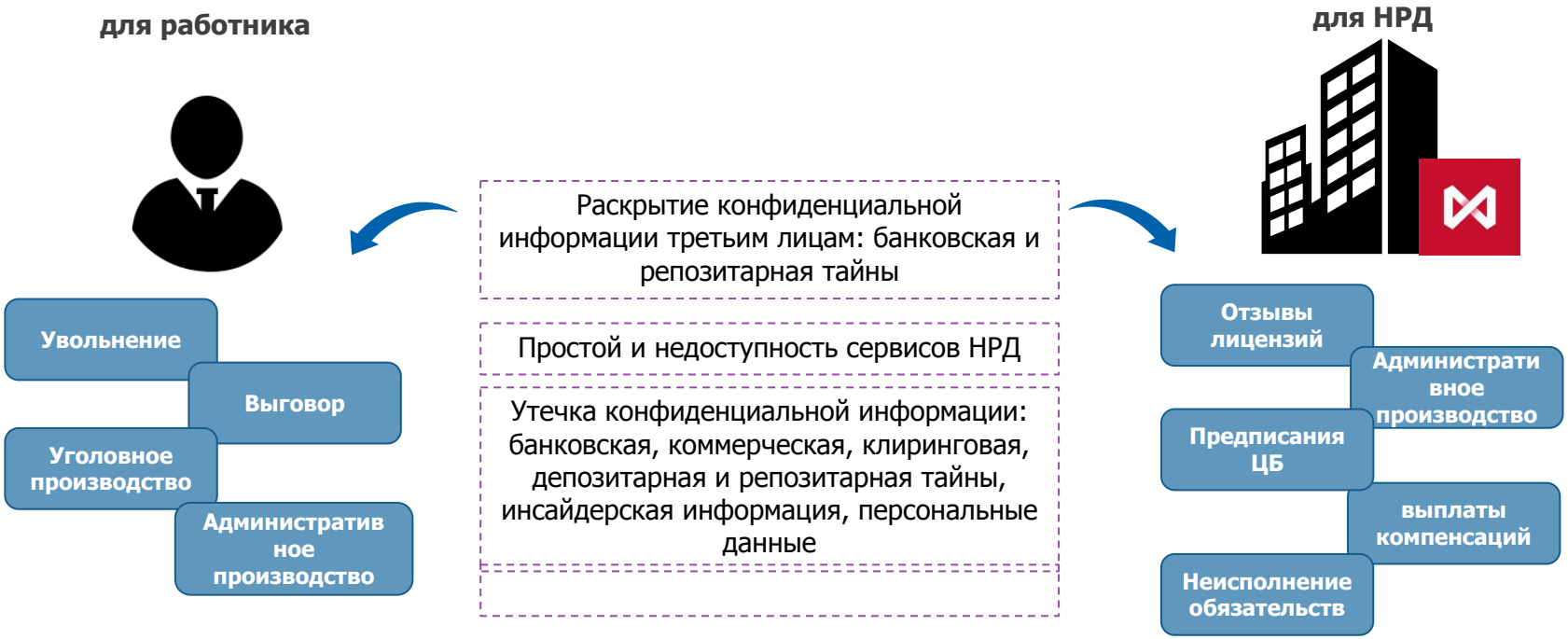
Грубые нарушения ИБ

- запись личных идентификаторов и паролей для входа в программы и операционные системы на носителях информации, доступных другим лицам;
- передача своих персональных идентификаторов и паролей кому бы то ни было;
- самостоятельное предоставление доступа по сети к ресурсам своего компьютера;
- регистрация и работа в системе под чужим идентификатором и паролем, за исключением случаев, когда действуют общие (групповые) идентификаторы;

- игнорирование системных сообщений и предупреждений об ошибках;
- самостоятельная установка на автоматизированные рабочие места программных и аппаратных компонентов и устройств, если иное не определено должностной инструкцией или специальным разрешением руководства (заявка);
- удаление, блокировка или самостоятельная замена антивирусных программ;
- копирование на съёмные носители любого программного обеспечения и файловых данных, если этого не требует технология рабочего процесса;
- открытие вложений и переход по ссылкам в электронных сообщениях от неопознанных источников и/или неизвестного назначения.
- целенаправленный обход установленных ограничений, обход средств защиты, повышение привилегий без соответствующих заявок.

Контроль и ответственность

В целях предотвращения утечек данных и защиты от вредоносного ПО НРД осуществляет **протоколирование и анализ всего трафика** и всех действий пользователя.
Трафик с сетью Интернет терминируется и расшифровывается (за исключением wi-fi сети и доверенных ресурсов, таких как системы ДБО). Все работники НРД должны понимать это и использовать офисные сети НРД только в рабочих целях.
Каждый работник несет **персональную ответственность** за действия, совершенные им, а также за действия, совершенные с использованием его учетных данных (кроме случаев, если будет доказана утечка этих данных в условиях соблюдения работником Политик ИБ).
Рассмотрим возможные последствия для Компании и для работника в случае нарушения Правил ИБ и законодательства в части обеспечения информационной безопасности конфиденциальной информации на примере некоторых нарушений:



Контакты Управления ИБ

Общий почтовый адрес УИБ

iss@nsd.ru

любой сотрудник УИБ доступен по почте и телефону, указанным в телефонном справочнике на **intra.nsd.ru**

Дежурный администратор УИБ

вн. тел.: 4900

с 8:00 до 21:00

СПАСИБО
ЗА ВНИМАНИЕ!

Желаем успехов в изучении материалов и прохождении тестов!