

**Правила и требования  
информационной  
безопасности**

# Не попадайте под обманы

Преступники и мошенники непрерывно изобретают новые схемы предназначенные для компрометации компьютеров, кражи паролей, обмана пользователей для раскрытия ценной информации, часто с целью завладения денег. В связи с этим необходимо быть осведомленным, какие методы мошенники могут использовать против вас.

## МОШЕННИКОВ!

Социальная инженерия — это метод несанкционированного доступа к информации или системам хранения информации без использования технических средств.

**Метод основан на использовании слабостей человеческого фактора** и является очень эффективным.

Злоумышленник получает информацию, например, путем сбора информации о служащих объекта атаки, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

### ОСНОВНЫЕ ПОКАЗАТЕЛИ МОШЕННИЧЕСТВА

1. Неожиданное письмо со ссылкой или вложением
2. Запрос личной или другой приватной информации, например пароль или информацию о финансовом счете
3. Использование тактики - если вы не будете действовать быстро, произойдет что-то плохое
4. Обещания чего-то слишком хорошего - сделки и «отличные предложения», или ссылки для получения вознаграждения
5. Просьба переслать вложения, ссылки и т.д. своим друзьям, коллегам или родственникам

**Фишинг** - это мошенничество, целью которого является кража информации или паролей, компрометация компьютеров и другого обмана для завладения финансов. Как правило, фишинг осуществляется через обманчивые электронные письма, сообщения на сайтах социальных сетей, всплывающие окна или телефонные звонки. **Мошенник, который использует метод фишинга может запрашивать ваше имя, учетные данные (логин и пароль), дату рождения, адрес и другое.** Они также могут попытаться заставить вас перейти по ссылке или открыть файл.

Письмо не адресовано вам, в частности, по имени

Письмо содержит орфографические или грамматические ошибки

Письмо содержит вложение с неправильным или подозрительным именем файла, файл с подозрительным расширением (например: \*.zip, \*.exe, \*.vbs)

Письмо включает ссылки на фотографии или видеоролики людей, которых Вы лично не знаете

# КАК ЗАЩИТИТЬ СЕБЯ?

**1** Не открывайте подозрительные вложенные в email файлы и не переходите по ссылкам если не уверены в подлинности отправителя!

**2** Удаляйте спам и подозрительные письма, не пересылайте и не отвечайте на них.

**3** Не нажимайте ссылки на всплывающие объявления / окна

**4** Никогда и никому не сообщайте свой пароль, даже если собеседник представляется сотрудником ИТ-подразделения, представителем вашего банка и т.д.

**5** Не предоставляйте персональную и конфиденциальную информацию незнакомым людям.

**9** Если вы не можете проверить, является ли письмо законным - сообщите в Департамент ИТ безопасности

**7** Не передавайте конфиденциальную информацию через публичные мессенджеры!

**8** Устанавливайте программное обеспечение только по запросам в Service Desk

**6** Не храните конфиденциальную информацию на съемных носителях или публичных облачных хранилищах

# Парольная

## Почему пароли должны защищаться и быть надежными?

Завладевние злоумышленником вашим паролем может привести к следующим угрозам:

- получения доступа к вашему компьютеру или мобильному устройству и к данным на нем
- авторизации транзакции без вашего ведома
- получения доступа к программам, файлам и приложениям, к которым доступ должен быть ограничен
- смену пароля

## Требования к созданию и хранению паролей

1. Пароли должны содержать минимум восемь символов, и как минимум 3 из 4 наборов символов: маленькие латинские буквы, большие латинские буквы, цифры и символы. **Обратите внимание, чем больше длина пароля, тем меньше он подвергнут риску взлома! Согласно рекомендациям международных организаций в сфере информационной безопасности надежный пароль - это не просто одно слово, а определенная фраза, словосочетание, или даже предложение.**
2. Запрещено использовать в качестве пароля имена ваших родственников или близких, даты рождения, имя домашнего питомца и и другие комбинации, которые могут быть легко угадываемыми.
3. Используйте разные пароли для разных систем, а так же разные пароли для личных и корпоративных ресурсов.
4. Не используйте в качестве паролей примеры, которые вы видели на публичных страницах.
5. Новый пароль не должен совпадать с 24 предыдущими.

## Защитите свои пароли

- ✓ Не раскрывайте свои пароли никому, даже сотрудникам технической поддержки и руководителям
- ✓ Не записывайте свои пароли
- ✓ Для хранения паролей используйте корпоративный менеджер паролей PMP
- ✓ Не храните свои пароли в текстовом документе на своем компьютере
- ✓ Всегда изменяйте пароли по умолчанию при первом входе в систему. Эти пароли могут быть особенно уязвимы для угадывания или взлома.
- ✓ Убедитесь, что пароли передаются надежно - перед тем, как войти на веб-сайт, найдите «https» (а не http) в URL-адресе, чтобы убедиться, что существует безопасное соединение.

# Конфиденциальная информация и персональные данные

**Для того, чтобы защитить данные с ограниченным доступом должным образом каждый сотрудник компании должен понимать с каким типом информации работает.**

## Конфиденциальная информация это:

- сведения, в том числе коммерческая тайна, ноу-хау и персональные данные, имеющие действительную или потенциальную коммерческую ценность в силу их неизвестности третьим лицам, к ним нет свободного доступа на законном основании, и компания принимает меры к охране их конфиденциальности
- информация, связанная прямо или косвенно с правоотношениями сотрудника компании
- деловые и коммерческие данные о компании, ноу-хау, формулы, процессы, разработки, эскизы, фотографии, планы, рисунки, технические требования, отчеты, модели, списки клиентов, прайс-листы, исследования, полученные данные, компьютерные программы, изобретения, идеи, а также информацию, касающуюся образцов, опытных образцов, моделей, маркетинга или рекламирования любого продукта, услуг, деловой политики, бизнес-планов или практики деловых отношений
- информация, полученная от третьих лиц, которую компания обязана рассматривать, как конфиденциальную
- любые производные, которые могут быть созданы сотрудником компании в результате изменения полученной информации путем улучшения, перевода, ограничения, адаптации или любого другого изменения конфиденциальной информации, включающего без ограничения отчеты, тесты или оценочные результаты

**Персональные данные** это любая информация, которая относится к определенному физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация;

**к персональным данным также относятся сведения о сотрудниках компании, сведения о личных данных физических лиц, которые являются клиентами или контрагентами компании**

**Коммерческая тайна** это защищаемые компанией сведения в области ее коммерческой деятельности, распространение которых может нанести убытки компании. Коммерческая тайна может быть представлена в виде результатов интеллектуальной деятельности (ноу-хау), а также в виде информации, не содержащей результатов творческой деятельности, но предназначенной для ограниченного круга лиц, включающей первичные бухгалтерские документы и промежуточные финансовые отчеты; сведения о наиболее выгодных формах использования денежных средств, ценных бумаг, акций; деловую переписку; списки клиентов; сведения о заключенных соглашениях, их содержании, предложения по их заключению; планы развития и реорганизации производства; структуры и методы управления; связи внутри и вне компании; распределение должностных обязанностей и их содержание; кадровый состав, его подбор, формирование; иную информацию, не подпадающую под определенный законом и иными правовыми актами перечень сведений, которые не могут составлять коммерческую тайну.

# Политика чистого стола и чистого экрана



1. Всегда закрывайте активные сеансы по завершении работы
2. Блокируйте экран компьютера, если покидаете рабочее место
3. По завершении работы материальные носители запирайте в сейф или шкаф
4. Документы, содержащие конфиденциальную информацию, должны немедленно удаляться с принтеров, при завершении печати
5. В конце рабочего дня приведите в порядок рабочий стол и уберите все офисные документы в запираемый шкаф или сейф
6. Для утилизации конфиденциальных документов используйте надежный метод - уничтожители бумаги или порвите документ на мелкие части.

# Уведомление об инцидентах информационной безопасности

**Инцидент информационной безопасности** - это попытка или успешный несанкционированный доступ в сеть компании, раскрытие информации, неправильное использование информационных систем, сетей или данных, включая кражу и взлом.

Кража или потеря оборудования, которое содержит конфиденциальную информацию

Вредоносные программы и / или трафик

Попытки (неудачные или успешные) получить несанкционированный доступ к системе или ее данным

Скомпрометированная учетная запись пользователя

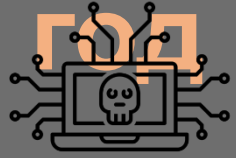
Реагирование на фишинговое письмо

Несанкционированное раскрытие конфиденциальной информации

Нарушения политик информационной безопасности Холдинга

**Если вы обнаружили инцидент информационной безопасности или подозреваете, что произошел инцидент - немедленно уведомьте своего руководителя и Департамент ИТ безопасности Холдинга (номер телефона - 00041, 00042, 00005: email - [itsecurity@bereggroup.com](mailto:itsecurity@bereggroup.com))**

# Инфографика по кибератакам за 2017



WannaCry/WannaCrypt

NotPetya/PetyaA

Bad Rabbit



Вирусы шифровальщики, вирусы вымогатели



12 мая 2017

27 июня 2017

24 октября 2017



Всемирная

Украина

Украина, Россия, Турция,  
Германия



Один из каналов заражения - открытие вредоносных файлов (документов Word, PDF-файлов), которые были направлены на электронные адреса пользователей

Первая волна заражения была воспроизведена через обновления бухгалтерского программного обеспечения М.Е.Дос , вторая - с помощью фишинговых электронных писем с вредоносными вложениями

Вирус распространялся через взломанные веб-сайты, предлагая пользователям установить обновление программного обеспечения Flash-player. После запуска загруженного файла вирус заражал устройство



# Документы Холдинга по требованиям информационной безопасности

## 1. Политика информационной безопасности

<https://conf.beregit.com/pages/viewpage.action?pageId=37060963>

## 2. Положение о защите конфиденциальной информации

<https://conf.beregit.com/pages/viewpage.action?pageId=38047673>

## 3. Положение о парольной защите

<https://conf.beregit.com/pages/viewpage.action?pageId=40668311>

## 4. Положение об использовании корпоративной почтовой системы на личных мобильных устройствах

<https://conf.beregit.com/pages/viewpage.action?pageId=40668319>

## 5. Руководство про порядок безопасного использования почтовых ресурсов и сети Интернет

<https://conf.beregit.com/pages/viewpage.action?pageId=40668315>

## 6. Процедура предоставления доступа в Confluence

<https://conf.beregit.com/pages/viewpage.action?pageId=40668327>

## 7. Процедура предоставления доступа в Интернет

<https://conf.beregit.com/pages/viewpage.action?pageId=35522328>