Повышение осведомленности сотрудников в области Информационной безопасности

Основы обеспечения информационной безопасности РГПУ им. А. И. Герцена

Курс подготовил:
Ведущий инженер отдела информационной безопасности управления информатизации РГПУ им. А. И. Герцена
Новик Георгий Дмитриевич

Управление информатизации

Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219

Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00

Телефон/факс: (812) 314-41-09

Электронная почта: ui@herzen.spb.ru

Список сокращений

ИБ - Информационная безопасность
ВУЗ -высшее учебное заведение
ИС – информационная система
ПДн – персональные данные
ИС ПДн – информационная система персональных данных
АРМ – автоматизированное рабочее место
ПК – персональный компьютер
ПО – программное обеспечение
ЭЦП – электронная цифровая подпись
СКЗИ - средство криптографической защиты информации
ЕИС - Единый идентификатор сотрудника

Для чего этот курс?

- В связи с резким обострением международной обстановки
- В связи с повышением вероятности информационных угроз
- В связи с увеличением количества спам сообщений, с вредоносными ссылками

Почему мы проводим эту работу с сотрудниками?

- В ВУЗе происходит обработка большого массива ПДн абитуриентов, студентов и сотрудников университета.
- Потенциально высокий урон при инцидентах информационной безопасности при обработке ПДн

Информационная безопасность

- Каждое высшее учебное заведение (ВУЗ) является оператором персональных данных (ПДн) .

- Защита Информационной системы персональных данных (ИС ПДн) ВУЗа является одной из наиболее актуальных и сложных задач в области информационной безопасности.

Информационная безопасность (ИБ) – это процесс, направленный на обеспечение:

- Конфиденциальности
- Целостности
- Доступности

…информации

Для чего информационная безопасность нужна?

Работа по обеспечению информационной безопасности проводится управлением информатизации РГПУ им. А. И. Герцена для профилактики угроз информационной безопасности, выполнения норм законодательства.

Под угрозой информационной безопасности понимается потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, доступности или конфиденциальности информации.

По России:

- Основная часть утечек – это персональные данные (ПДн 85,2%)

- Основная причина утечек – это невнимательность пользователей организации (88,2%)

Из за каких действий пользователя АРМ может быть нарушена информационная безопасность?

- Ненадлежащая парольная защита
- Проблемы с антивирусным ПО
- Отсутствие бдительности при работе в интернете
- Ошибки при работе с PDF документами
- Передача данных через внешнюю почту, мессенджеры
- Небрежное отношение к сохранности информации
- Небрежное отношением к ЭЦП
- Невнимательная работа в 1С Документооборот
- Неправильная организация АРМ с точки зрения ИБ

Средства защиты информации в ВУЗе

Технические

- Межсетевой экран, подсети
- Сохранность и доступность,
  резервное копирование данных
- Спам-фильтры и антивирус в почте
- Антивирус на ПК, агент администрирования

Правовые

Документы РГПУ имени А. И .Герцена в области информационной безопасности

РГПУ им. А.И. Герцена → Общий → Структура → Управления университета → Управление информатизации → Отдел информационной безопасности → Нормативные документы по обеспечению информационной безопасности

Физические

- Ограничение доступа на территорию
- Разграничение доступа в помещения
- Организационные мероприятия =>
  Разъяснительная работа с персоналом

Криптографические

ЭЦП

Шифрование данных

Организация парольной защиты

Количество знаков	Количество вариантов	Время перебора
1	36	менее секунды
2	1296	менее секунды
3	46 656	менее секунды
4	1 679 616	17 секунд
5	60 466 176	10 минут
6	2 176 782 336	6 часов
7	78 364 164 096	9 дней
8	2,821 109 9?1012	11 месяцев
9	1,015 599 5?1014	32 года
10	3,656 158 4?1015	1 162 года
11	1,316 217 0?1017	41 823 года
12	4,738 381 3?1018	1 505 615 лет

Требования к формированию паролей (часть 1):

- Длина пароля должна быть не менее 8 символов
- В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих: буквы в верхнем регистре; буквы в нижнем регистре; цифры не более 50%; специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, *, % и т.п.).
- Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).
- Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.
- Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

Организация парольной защиты

- Личные пароли должны создаваться пользователями самостоятельно.
- Плановую смену пароля рекомендуется проводить не реже одного раза в 3 месяца.
- После окончания работы, рекомендуется включить блокировку экрана АРМ
- Не рекомендуется хранить записи о логинах и паролях в доступном месте (например, на мониторе)
- Не рекомендуется использовать один и тот же пароль в разных учётных записях (например, почта и банковская карта)

Требования к формированию паролей (часть 2):

- При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях (например, Gjhjlf0385 => geltkM0485).
- НЕ РЕКОМЕНДУЕТСЯ использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).
- НЕ РЕКОМЕНДУЕТСЯ использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

Плохие пароли	Хорошие пароли
123456789	D)dzq4Smo@
password	4j~8GvG{qB
qwerty	Re18ZEVH1#
master	Hx4@5g8DoJ
login1	%FfZMv4vDu
1a2s3d4f5g	pWjtbQ$g6B

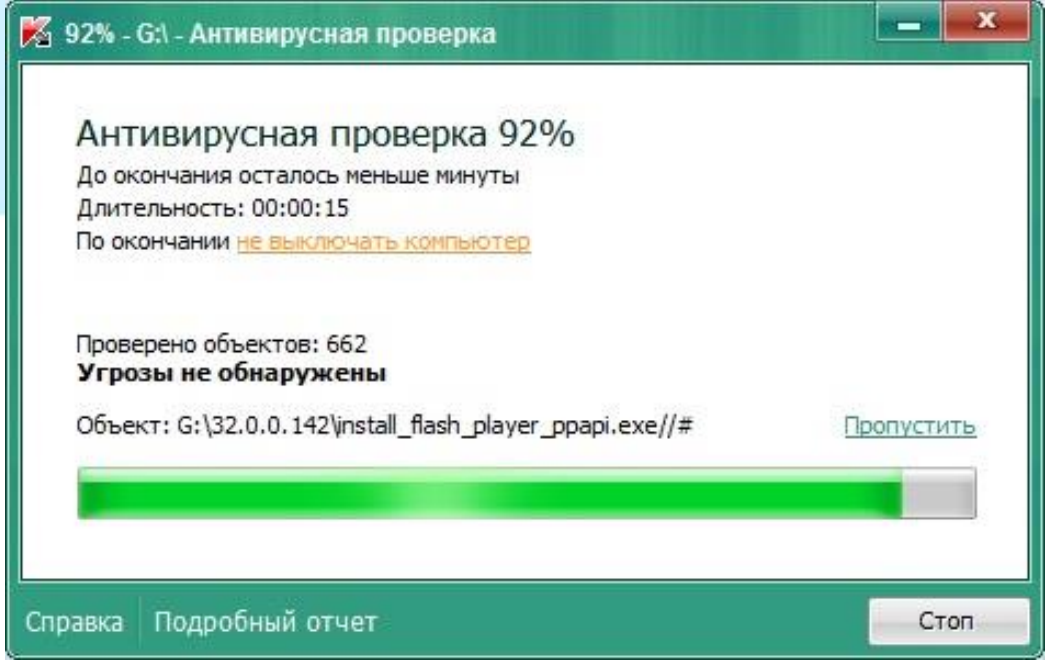
Последствия.

Соблюдать рекомендации чрезвычайно важно, так как злоумышленник может получить доступ к:

- паролю от Вашего АРМ
- всем настройкам АРМ
- рабочим и личным данным на АРМ
- сетевым дискам
- всем паролям, сохраненным в браузере
- всем аккаунтам (Гугл/Яндекс)аккаунтов
- всем сервисам (социальные сети, мессенджеры)
- личной информации (переписка, фотографии)
- истории браузера, всех действий пользователя и истории его местоположений.

В результате действий злоумышленника может пострадать Работник, а также может быть украдена, уничтожена, намеренно искажена конфиденциальная информация, что нарушит законодательство и может привести к проблемам работы РГПУ им. А. И. Герцена.

Работа с антивирусным ПО



Антивирусное ПО работает под управлением программы «Агент администрирования» установленной управлением информатизации РГПУ им. А. И. Герцена, что обеспечивает:

- автоматически, в соответствие с расписанием, плановую проверку АРМ на вредоносное ПО.
- автоматически, в соответствие с расписанием, обновление базы вирусов.
- Автоматическую проверку подключенных накопителей информации.

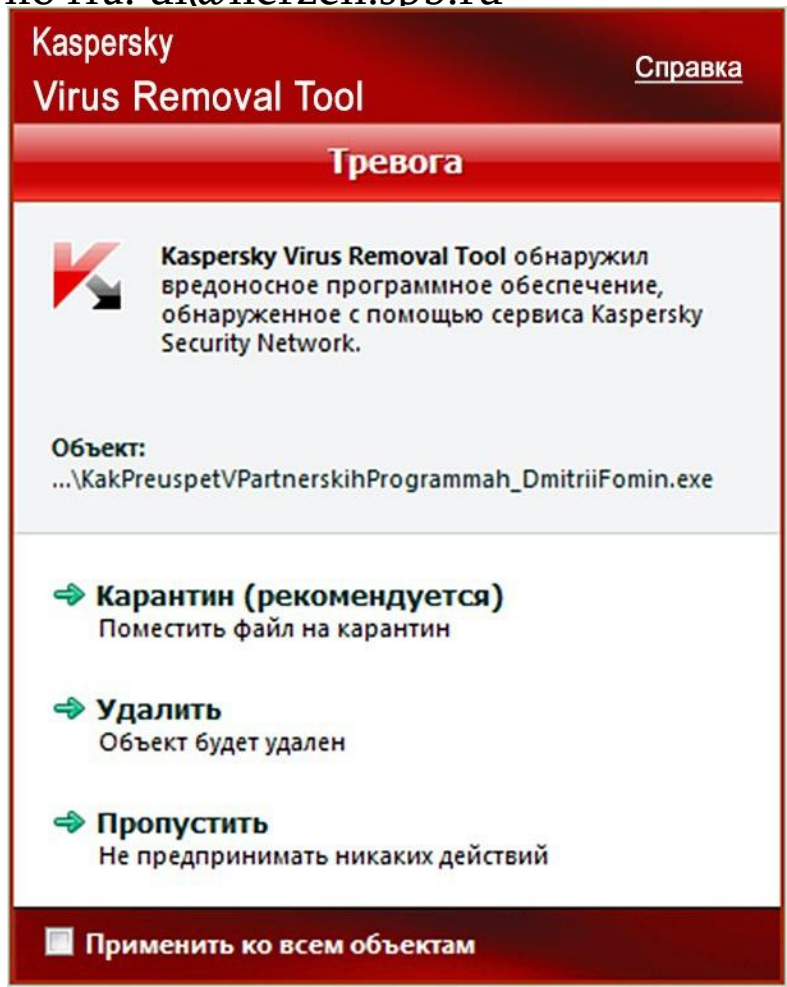
Настоятельно рекомендуется не вмешиваться в работу Антивирусного ПО, не прерывать автоматическую проверку подключенных накопителей информации.

Ситуации, угрожающие АРМ:

- Отсутствие антивирусного ПО
- Окончание срока действия лицензии на антивирусное ПО
- Заражение, с которым не смогло справиться антивирусное ПО

В случае угрожающей ситуации настоятельно рекомендуется обратиться в управление информатизации РГПУ им. А. И. Герцена.

Управление информатизации
Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219
Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00
Телефон/факс: (812) 314-41-09
Электронная почта: ui@herzen.spb.ru

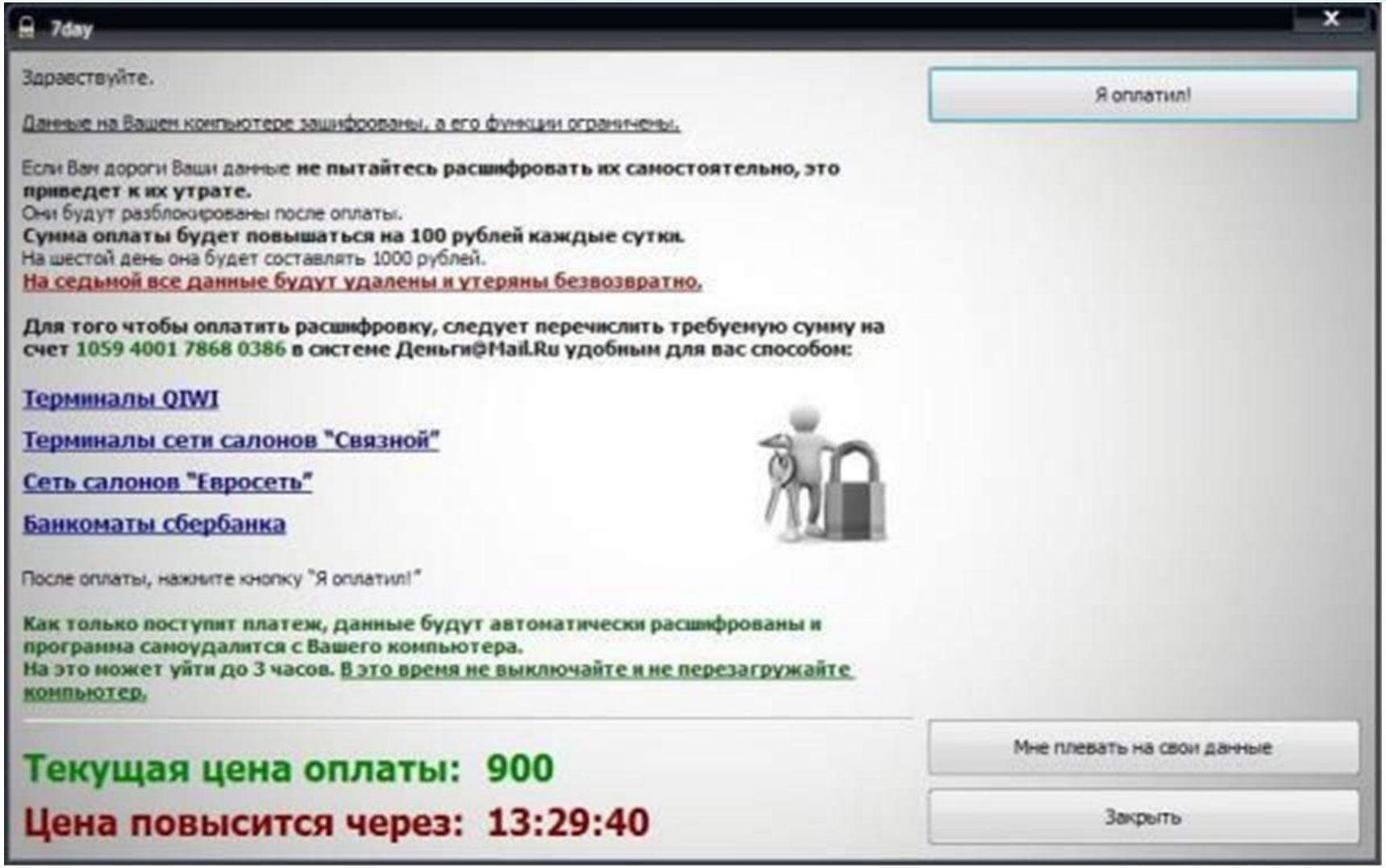


Последствия.

Вредоносное ПО может:
- собирать
- красть
- шифровать
- уничтожать

любую информацию.

Последствия заражения АРМ вредоносным ПО могут различаться - от замедления работы АРМ до полного обрушения системы с потерей всех файлов на АРМ.



Интернет

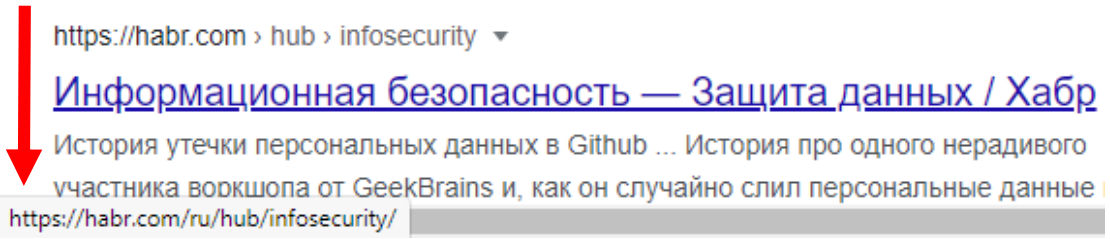
При работе в сети интернет нужно проявлять:

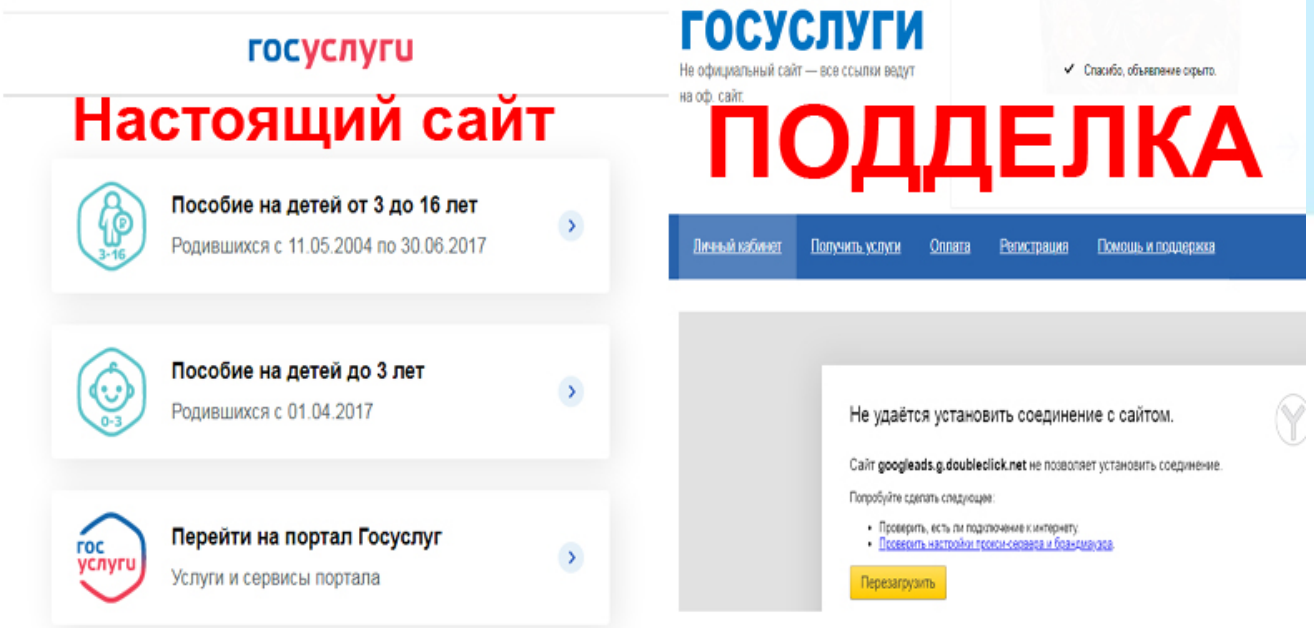
Внимательность и осознанность.

- **Необходимо внимательно относиться к предупреждениям браузера о небезопасном сайте.** Скорее всего сайт, который Вы пытаетесь посетить, заражен и распространяет вредоносное ПО.

Интернет

При работе в сети интернет нужно проявлять: Внимательность, осознанность





Настоящий сайт ГОСУСЛУГ пишется — gosuslugi.ru
Фальшивый имеет окончание s — gosuslugis.ru

- **Необходимо следить за адресами, на которые ведут ссылки.** Для того чтобы узнать адрес, на который ведет ссылка необходимо просто навести на нее курсор. Если вам предлагают перейти на сайт X, а ссылка ведет на сайт Y то тут что-то не так. Возможно, вас пытаются обмануть.
- **Перед вводом личной информации проверяйте адресную строку браузера.** Если вы там увидите что то вроде https://www.herzen.spd.ru/ вместо привычного https://www.herzen.spb.ru/, то можете быть уверены, что вы находитесь на поддельном сайте и у вас пытаются украсть пароль для доступа к вашему аккаунту.

Интернет

При работе в сети интернет нужно проявлять:
Внимательность
Осознанность

- **Не кликайте по подозрительным рекламным баннерам**, предлагающим мгновенное обогащение или другие **очень** выгодные услуги и сервисы. Скорее всего, Вас пытаются обмануть.

- **Будьте внимательны к файлам загружаемых через BitTorrent**, DirectConnect и другие файлообменные сети. Пользователи данных сетей могут распространять вирусы, даже не подозревая об этом.

- **Никогда сразу не открывайте файлы, скачанные из интернета**, почтовые вложения. Проверьте их сначала с помощью антивирусного ПО.

Интернет и почта

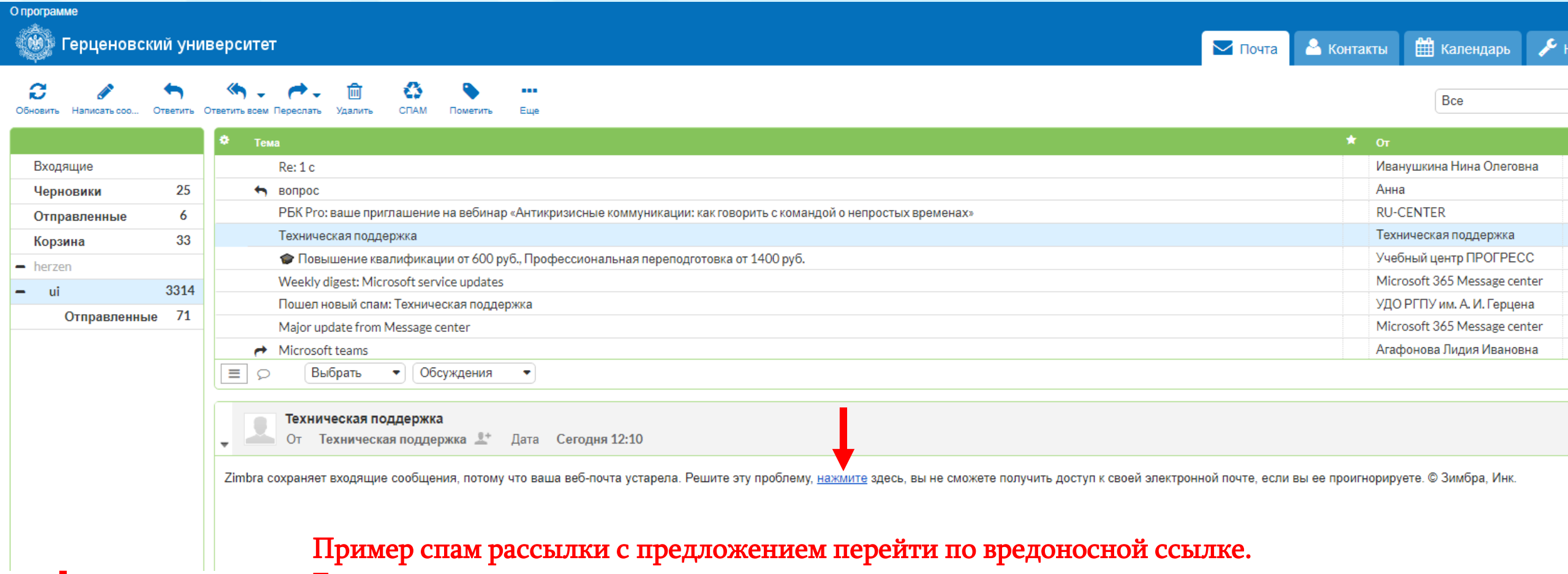
При работе в сети интернет нужно проявлять:
Внимательность
Осознанность

- **Не переходите по незнакомым ссылкам, которые приходят вам на почту, или в социальные сети**. Даже если ссылка пришла от знакомого Вам адреса необходимо быть максимально внимательным. Вполне возможно, данный адрес просто похож на знакомый Вам (например «Финансовый отдел» и пр.) или взломан, и теперь злоумышленники от его имени рассылают вредоносное ПО.

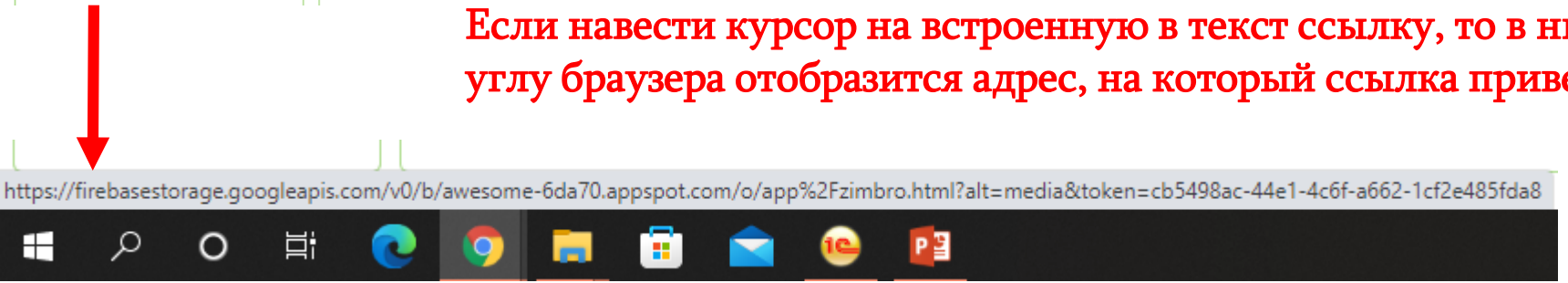
- **Не скачивайте неизвестные файлы, пришедшие вам на почту** или в мессенджер или социальную сеть, даже если файл пришел со знакомого Вам адреса. Перед тем как скачивать такие файлы уточните у отправителя, что это за файл.

Интернет и почта

При работе в сети интернет нужно проявлять:
Внимательность
Осознанность



Пример спам рассылки с предложением перейти по вредоносной ссылке.
Если навести курсор на встроенную в текст ссылку, то в нижнем левом углу браузера отобразится адрес, на который ссылка приведёт.

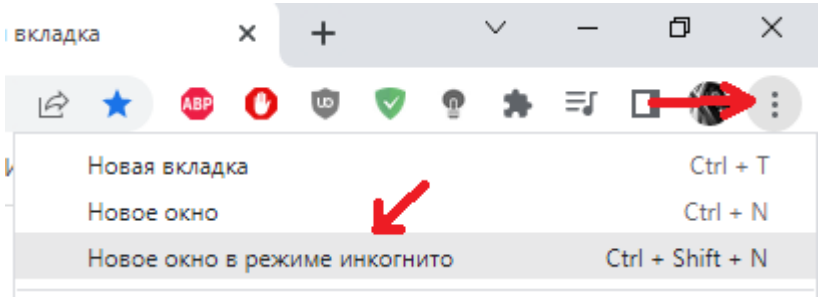


Интернет и данные

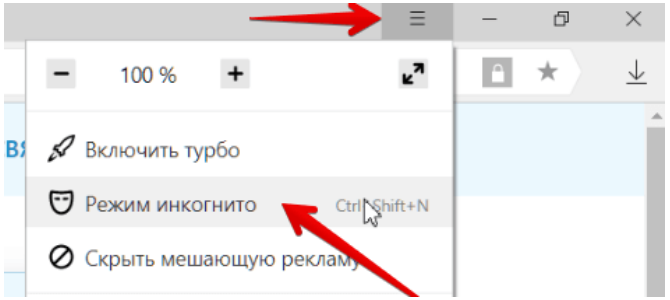
- Браузер сохраняет **ВСЕ** Ваши действия
- При заходе в свою учетную запись (Google, Яндекс, Apple) с чужого ПК, **ВСЕГДА** выходите из неё перед уходом.

- По возможности на чужом ПК рекомендуется работать с режима инкогнито
- Режим инкогнито включается одновременным нажатием клавиш: Ctrl + Shift + N.

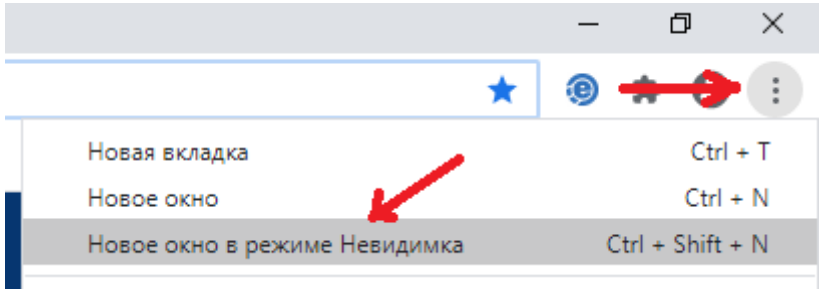
Google Chrome



Яндекс.Браузер



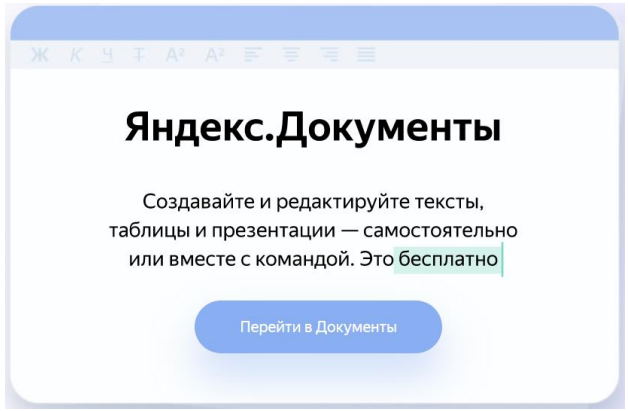
Спутник



Интернет и данные

В связи с обострением в международных отношениях, увеличилась вероятность отключения / блокировки зарубежных сетевых хранилищ

=>



Яндекс Диск

Рекомендуется использование отечественных сервисов, где сервера находятся на территории РФ

Ошибки при работе с PDF файлами, приводящие к утечке данных

Проблема PDF:

Преобразование в PDF формат / сжатие PDF документов зачастую производится в онлайн-конвертерах.
Происходит утечка данных на зарубежные сервера.

Рекомендуется использовать локальные PDF приложения

PDF24:

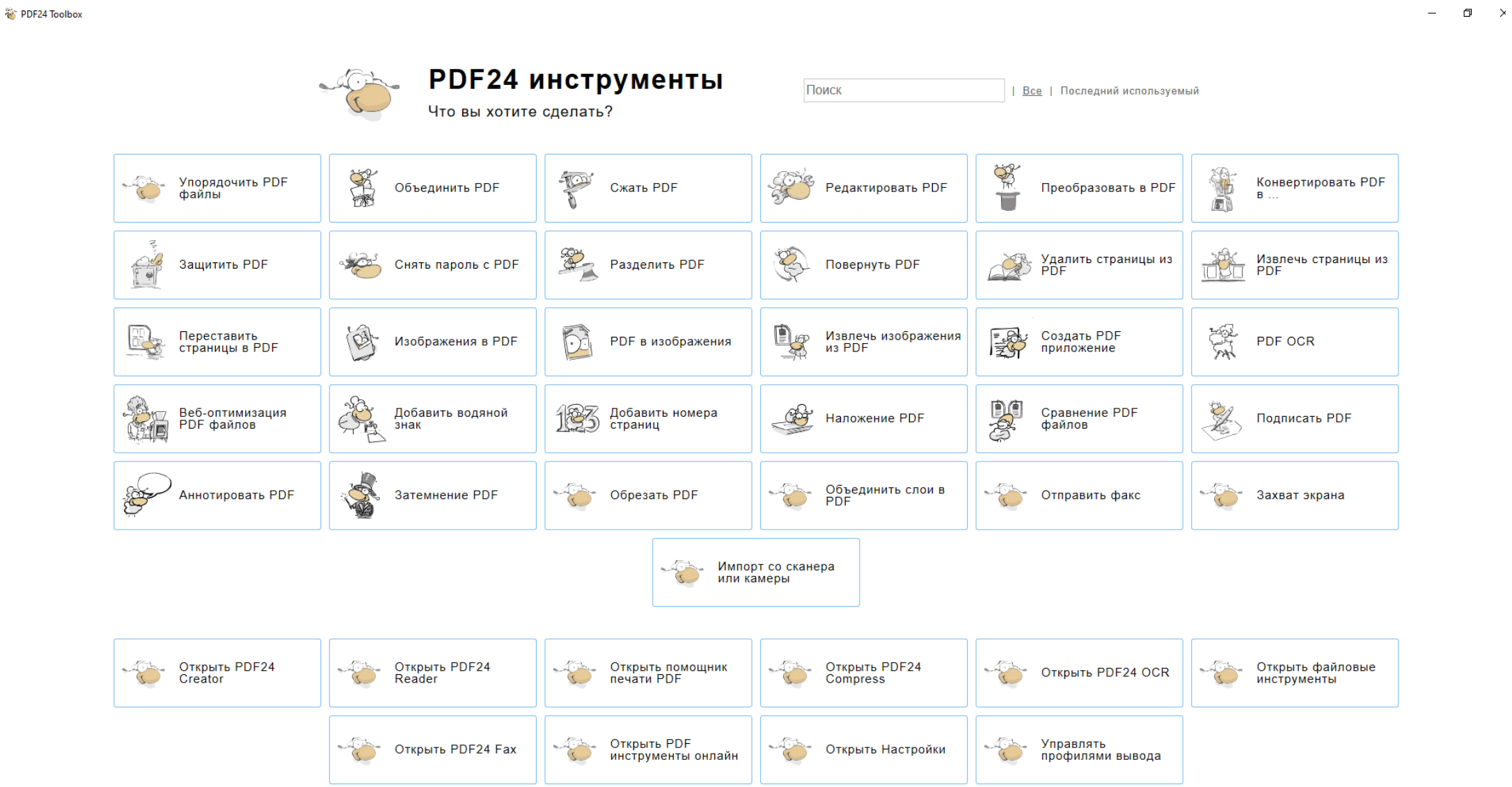
- Прост в использовании
- Бесплатен
- Безопасен
- Положительный опыт применения в приемную кампанию 2021

Где взять?

- Управление информатизации
- Официальный сайт https://ru.pdf24.org/

Управление информатизации
Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219
Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00
Телефон/факс: (812) 314-41-09
Электронная почта: ui@herzen.spb.ru

Рабочий функционал PDF24



Передача персональных данных

- Утечка данных может происходить через внешнюю почту (gmail, yahoo и др.) и мессенджеры.

- Управление информатизации прорабатывает варианты перехода с WhatsUpp и других мессенджеров на систему передачи данных внутри организации.

ЭЦП. Правила безопасности

Основная доля рисков для пользователя ЭЦП связана с недостаточно ответственным отношением к обращению с носителем закрытого ключа. Большая часть преступлений с использованием электронной подписи связана с компрометацией её закрытого ключа, хранить который в тайне —обязанность пользователя ЭЦП.

Главные правила пользователя:

не передавать другим людям свой носитель ЭЦП

не терять носитель ЭЦП

не оставлять в доступности посторонних лиц

В Федеральном законе от 06.04.2011 №63-ФЗ «Об электронной подписи» говорится о том, что участники взаимодействия с применением ЭП не должны допускать использования своей электронной подписи другими лицами.

ЭЦП. Правила безопасности

Должно быть исключено бесконтрольное проникновение и пребывание в помещениях, посторонних лиц. В случае необходимости присутствия таких лиц в указанных помещениях должен быть обеспечен контроль за их действиями.

Должно быть исключен не санкционированный доступ к ПК пользователя ЭЦП (как физическое, так и техническое), также не допускается оставлять без контроля АРМ при включенном питании и загруженном программном обеспечении СКЗИ после ввода ключевой информации.

Для этого требуется выполнять инструкции в разделах:

- Пароль
- Антивирус
- Интернет
- Почта

Последствия.

Управление информатизации
Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219
Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00
Телефон/факс: (812) 314-41-09
Электронная почта: ui@herzen.spb.ru

В случае компрометации ключа ЭЦП или несанкционированного доступа к средствам ЭЦП может быть создан / изменен / получен документ, порождающий юридически значимые последствия и исходящий от имени пользователя, ключ которого был скомпрометирован.

В случае нештатной ситуации с ЭЦП (подозрения на несанкционированный доступ к ЭЦП или компрометации ЭЦП), настоятельно рекомендуем обратиться в управление информатизации РГПУ им. А. И. Герцена.

Сохранность информации

Управление информатизации
Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219
Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00
Телефон/факс: (812) 314-41-09
Электронная почта: ui@herzen.spb.ru

Часто случаются ситуации, когда Работник хранит на АРМ большой массив данных за много лет работы. И в случаях, когда АРМ выходит из строя, есть вероятность потерять огромное количество критически важных данных.

С целью сохранности информации рекомендуется:

- Дублировать важную информацию на съемные носители
- Хранить информацию на сетевых дисках РГПУ им. А. И. Герцена
- При признаках неисправности ПК обратиться в управление информатизации РГПУ им. А. И. Герцена

Сетевые диски

Сетевые диски автоматически проводят резервное копирование данных каждую ночь.

Пользователь АРМ должен:

- Не допустить компрометацию пароля.
- Исключить доступ посторонних лиц к сетевым дискам отдела студентов.
- С осторожностью работать с документами на сетевых дисках. Не «удалять», не «вырезать».

В случае нештатной ситуации (разрыва соединения с сетевым диском или уничтожения информации или компрометации пароля) рекомендуется обратиться в управление информатизации РГПУ им. А. И. Герцена.

Управление информатизации
Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219
Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00
Телефон/факс: (812) 314-41-09
Электронная почта: ui@herzen.spb.ru

1С Документооборот

- Рекомендуется работать в 1С через клиент, а не web
- С целью предотвращения утечки документов рекомендуется внимательностью относиться к адресату, которому отправляется документ.
- Необходимо исключить компрометацию пароля

В случае нештатной ситуации (разрыва соединения с 1С Документооборот или компрометации пароля) настоятельно рекомендуется обратиться в управление информатизации РГПУ им. А. И. Герцена.

Управление информатизации
Санкт-Петербург, наб. р. Мойки, д.48, корп. 1, ауд. 219
Ежедневно с 9.00 до 18.00, обед с 13.00 до 14.00
Телефон/факс: (812) 314-41-09
Электронная почта: ui@herzen.spb.ru

Организация АРМ с точки зрения информационной безопасности

При организации рабочего места важно учитывать следующие аспекты:

- Монитор должен располагаться так, чтобы исключить возможность чтения с него конфиденциальных данных посетителем.
- Нельзя оставлять на рабочем месте пометки с логинами и паролями от учетных данных информационных систем университета, АРМ, почты и пр.
- Бумажные документы на рабочем столе должны располагаться так, чтобы исключить возможность их чтения посетителем.

Зарубежные Операционные системы

В связи с санкционной политикой стран Евросоюза и США, нельзя исключать вероятность прекращения сотрудничества в сфере IT, в том числе – в сфере продаж программного обеспечения.

Windows

Производитель - Microsoft

+:Стабильная и надежная

+:87% мирового рынка, все решения заточены под неё

+:Все пользователи знакомы с данной ОС

-: Не безопасная – много вирусов. Антивирус обязателен

-:Слежка за пользователем

-:Постепенный переход на «платные» решения

-: Неизвестны перспективы работы в РФ

Mac OS

Производитель - Apple

+:Стабильная, лаконичная, красивая, продуманная

+:Безопасна – мало вирусов

+:Хорошо оптимизирована внутри экосистемы

-: Платная экосистема

-: Ограниченность. Нет гибкости в настройках

-:Слежка за пользователем

-:9,2% мирового рынка, проблемы с поддержкой оборудования

-:Неизвестны перспективы работы в РФ

Linux Ubuntu

Производитель - Canonical

+:Стабильная и надежная

+:Самая распространенная Linux система

-: Большинство пользователей не знакомы с данной ОС

-: Проблемы с массовым переходом пользователей – нужно обучение

-:Проблемы с совместимостью ПО и оборудования

Linux Mint

Производитель - Mint Linux Team + сообщество пользователей

+:Стабильная и надежная

+:Улучшенная версия Ubuntu

+:Оптимизирована под пользователя

-: Большинство пользователей не знакомы с данной ОС

-: Проблемы с массовым переходом пользователей – нужно обучение

-:Проблемы с совместимостью ПО и оборудования

Отечественные Операционные системы

Производитель – «Базальт СПО». Самая массовая ОС.

Производитель- «РЕД СОФТ» Заточена под легкую миграцию с ОС windows.

Производитель – «НТЦ ИТ РОСА». Заточена под безопасность в коммерческом секторе

Производитель – АО «НПО РусБИТех». Заточена под безопасность в государственных учреждениях.

ОС на базе Linux

+:Стабильные и надежные

+:Безопасны

+:Хорошие перспективы в рамках импортозамещения

-: Большинство пользователей не знакомы с данной ОС

-: Проблемы с массовым переходом пользователей – нужно обучение

-:Проблемы с совместимостью ПО и оборудования

Спасибо за внимание!

Курс подготовил:
Ведущий инженер отдела
информационной безопасности
управления информатизации
РГПУ им. А. И. Герцена
Новик Георгий Дмитриевич