каменный город

Ландарь Алексей Сергеевич

Руководитель федерального штаба проекта "Цифровая Россия"
Директор координационного центра по вопросам противодействия идеологии терроризма Минобрнауки РФ

Технический минимум безопасности

Основная архитектура внешней защиты информации – Ростелеком система ЕСПД.

- Маршрутизация (внешний файерволл для образовательной организации).
- Ограничение доступа к запрещённым ресурсам (экстремизм, заблокированные сервисы)
- Ограничение доступа к видеосервисам Google, Meta
- Ограничение на доступ систем VPN (протокол VLOSS)
- Блокировка доступа к незащищённым облачным сервисам

Внутренняя система защиты – ответственность учебного учреждения.

Основные угрозы:

- фишинг,
- подключение к внешним сетям,
- сохранение данных в иностранных облачных сервисах,
- использование подключения к файлообменным сетям и торрентам,
- использование VPN.

Обязательные элементы защиты

• Ограничение физического и программного доступа к серверу.
• Ролевой доступ во внутренней сети образовательного учреждения (личные пароли сотрудников).
• Антивирусная защита всех АРМ учреждения.
• Обучение сотрудников и просветительская работа по цифровой безопасности.
• Нормативное обеспечение цифровой безопасности внутри ОУ.

Антивирусы

Только отечественные сервисы (рекомендация):

1. Kaspersky Internet Security
2. Doctor Web
3. PRO32
4. NANO Антивирус Pro
5. 360 Total Security

Обучение сотрудников и просветительская работа

1. Курсы по цифровой безопасности для учителей (чем больше пройдут тем лучше);
2. Лекции от представителей региональных органов исполнительной власти в области цифровизации (у них есть внутренний KPI по цифровому просвещению);
3. Еженедельные планёрки с работниками с напоминанием о безопасных действиях в сети.

4. Краткая памятка для сотрудников

• Проверка электронной почты на вирусы, не открывать незнакомые файлы. Сразу удалять спам.

• Не пользоваться VPN

• Проверять флэш-носители антивирусом.

Нормативное обеспечение цифровой безопасности

1. Внутренний приказ по учреждению с утверждением ответственных лиц и разграничением полномочий.
2. Регламент реагирования на нештатные ситуации (заражение вирусом, потеря персональных данных, несанкционированный доступ, неработоспособность систем и оборудования);
3. Регламент действий в случае обнаружения экстремистских или террористических угроз (в учебных чатах, переписках, мессенджерах, электронной почте).
4. Утверждение официальных каналов передачи информации курирующим органам власти и правоохранительным органам.
5. Закрепление ответственности за нарушение регламентов и приказов.

Профилактика противоправного поведения детей

1. Противодействие идеологии терроризма и профилактика экстремизма – склонение несовершеннолетних к совершению особо тяжких преступлений (терроризм, нападение на органы власти, повреждение критически важных объектов).

2. Противодействие вовлечению несовершеннолетних в преступные сообщества
- Наркотики
- Мошеннические схемы (пароли родителей, доступ к смартфонам через игры)
- Онлайн-казино
- Нелегальные букмекеры (ставки на спорт)
- Продажа банковских карт

3. Чек лист по основным деструктивным направлениям (прилагается)
4. Принятие регламента в ОУ по профилактическому реагированию при обнаружении признаков поведения из чек-листа. Привлечение психологов и правоохранителей.
5. Базовая профилактика – объяснение детям рисков и что их цифровой след с ними навсегда. В интернете давно нет анонимности. Ответственность равна везде.

Потеря личных данных преподавателя (взлом аккаунта), что делать?

Как распознать взлом аккаунта?

1. Telegram просит войти заново. Если вы не выходили из аккаунта, но приложение внезапно требует ввести код, — это тревожный сигнал. Особенно если это произошло сразу на всех ваших устройствах. Такое бывает, когда взломщик вручную выходит из всех сессий, чтобы лишить вас контроля.
2. Сделан вход с незнакомых устройств. В Telegram можно посмотреть список устройств, где активен аккаунт. Зайдите в «Настройки», а затем — в «Устройства» (или «Активные сессии»). Если видите что-то незнакомое — это повод срочно действовать. Обратите внимание на модель устройства, IP-адрес и локацию.
3. Появились странные сообщения. Если от вашего имени начали приходить письма, которые вы не отправляли, — почти наверняка вас взломали. Обычно мошенники рассылают сообщения с просьбами перевести деньги, делятся подозрительными ссылками, спамят в группах или делают публикации в каналах, которые вы администрируете. Проверьте недавние чаты — и обратите внимание на реакцию собеседников.
4. Изменились настройки. Злоумышленники могут сменить имя или фото профиля, отключить двухфакторную защиту, изменить привязанный номер или email, перенастроить конфиденциальность. Если доступ ещё есть — проверьте, не изменилось ли что-то без вашего ведома.
5. Пришло уведомление о входе с нового устройства. Telegram сообщает о новых сессиях. Если вы не авторизовывались с другого гаджета, но получили такое сообщение, — стоит срочно проверить, кто вошёл.
6. Возникли проблемы с тем, чтобы получить или отправить сообщение. Взломщик мог изменить настройки, заблокировать кого-то или удалить чаты. Если сообщения не доходят или вдруг исчезли активные переписки — стоит насторожиться.
7. Заметили подозрительную активность ботов. Если вы используете ботов (особенно для платежей), проверьте историю их действий. Иногда мошенники действуют только через них.
8. Появились другие странные вещи в Telegram-канале, который вы ведёте. Это могут быть не только публикации, которые вы не размещали, но и изменения в описании канала, новые администраторы или удаление прежних. Также без видимой причины может резко увеличиться количество подписчиков.

Потеря личных данных преподавателя (взлом аккаунта), что делать?

Порядок действий при взломе аккаунта.

1. Войдите в свой аккаунт. Если вы всё ещё можете зайти в Telegram — это уже плюс. Если доступа нет, переходите сразу к пятому шагу.
2. Завершите все активные сессии. Это поможет разлогинить злоумышленника со всех устройств. Как это сделать: откройте в Telegram «Настройки», перейдите в «Устройства» и завершите все неизвестные сессии.
3. Смените пароль двухфакторной защиты (если она была включена). Для этого откройте в мессенджере «Настройки», перейдите в раздел «Конфиденциальность», а затем выберите «Облачный пароль». Измените пароль и убедитесь, что указан рабочий резервный email. Если двухфакторная аутентификация была выключена — не активируйте её сейчас. Сначала полностью восстановите доступ.
4. Напишите в поддержку Telegram, даже если вы уже восстановили доступ. Сообщить о взломе можно, написав на email: security@telegram.org. В письме укажите номер телефона в международном формате и опишите ситуацию: что случилось, какие шаги вы уже предприняли.
5. Если доступа к аккаунту нет — начните восстановление. Откройте Telegram и введите свой номер телефона, а затем — код из СМС. Если ваш номер был изменён — потребуется обратиться в поддержку Telegram. Подробнее об этом шаге рассказываем в следующем разделе статьи.
6. Проверьте и обновите настройки аккаунта. После восстановления доступа убедитесь, что злоумышленник ничего не изменил. Проверьте имя пользователя, фото профиля, номер телефона, email. Просмотрите настройки конфиденциальности, убедитесь, что нет посторонних активных сессий.
7. Расскажите контактам, что аккаунт был взломан. Напишите в личные чаты, группы и каналы, предупредите, чтобы игнорировали подозрительные сообщения от вас. Например, можно отправить такое письмо: «Мой аккаунт был взломан. Сейчас всё под контролем. Если от меня приходили странные сообщения — просто удалите их. Спасибо за понимание!»
8. Проверьте данные. Посмотрите, не отправлялись ли сообщения без вашего ведома, не были ли созданы новые группы или каналы, не исчезли ли важные переписки или файлы. Если что-то пропало — попробуйте восстановить. Для этого откройте «Настройки», нажмите «Дополнительно», а затем — «Экспорт данных».