Если после отпуска вы забыли свой пароль, отдых удался на славу.

А.В. Лукацкий

Информационная безопасность в образовательном учреждении

МАОУ ДПО ЦИТ,

Направления информационной безопасности

- Обеспечение защиты информационных систем общего назначения (локальной сети с подключением в Интернет и всех её составляющих: компьютеров, серверов, коммутаторов, точек беспроводного доступа, модемов, маршрутизаторов и пр.)
- Обеспечение защиты информационных систем персональных данных
- Обеспечение защиты детей от доступа к информации, несовместимой с целями образования

Обеспечение защиты информационных систем (ИС) общего назначения

- Определение и разграничение прав доступа в локальной сети
- Защита от несанкционированного доступа (НСД) к компонентам, составляющим ИС
- Защита от компьютерных атак
- Антивирусная защита
- Повышение надежности функционирования ИС

Определение и разграничение прав доступа в локальной сети

Компьютеры:

- Общего доступа (в кабинетах информатики, медиатеках, подключаемые по Wi-Fi, кабинетах открытого доступа). Фильтрация Интернет-контента, невозможность доступа к учительским и управленческим ПК, ИСПДн
- Учителей-предметников. Фильтрация Интернет-контента, невозможность доступа к управленческим ПК
- Управленческие (директора, завучей, делопроизводителя, бухгалтерии, медработника и т.п.). Наиболее защищаемый, «закрытый» для доступа извне сегмент

Серверы и активное оборудование:

- Группы доступа
- Централизованные ресурсы
- Резервное копирование

Защита от НСД к ИС

- Ограничение физического доступа
- Исполнение требований политики безопасности
- Контроль (аудит) действий пользователей
- Система обнаружения/предотвращения вторжений

Защита от компьютерных атак

- Отключение неиспользуемых сервисов
- Исполнение требований политики безопасности
- Система обнаружения/предотвращения вторжений
- Взаимодействие с провайдером
- Восстановление из резервной копии

Антивирусная защита

- Используемая версия должна поддерживаться производителем
- Обновление антивируса должно выполняться не реже одного раза в день
- Проверка содержимого носителя должна осуществляться перед началом работы с новым носителем и не реже раза в неделю с постоянно используемыми носителями
- Ни один антивирус не защитит Вас от Ваших же действий
- Ни один антивирус не заменит систему резервного копирования

Повышение надежности ИС

- Регламентные работы и техническое обслуживание серверов и ПК
- Обеспечение надежного электропитания компонентов ИС
- Жесткое регламентирование доступа, действий и зон ответственности
- Осуществление своевременного резервного копирования и тестирование восстановления
- Создание дублирующих ИС, блоков или ЗИП для наиболее критичных ИС
- Уменьшение влияния человеческого фактора

Обеспечение защиты ИСПДн

- Каждое ОУ является оператором ИСПДн и согласно ст. 19 ФЗ-152 должно проводить ряд мероприятий по защите ПДн, в т.ч. предоставлять регуляторам пакет документов на проверку http://66.rkn.gov.ru/p7598/p10408/
- С 01.09.2015 хранение ПДн россиян должно осуществляться на размещенных в России серверах
- Регуляторы: ФСБ, ФСТЭК, Роскомнадзор
- Проблема: отсутствуют нормативные акты, утверждающие форму типовых документов по защите ПДн в ОУ

Нормативные документы в области защиты ИСПДн

- Указ Президента Российской Федерации от 6 марта 1997 года №188 «Об утверждении перечня сведений конфиденциального характера».
- Федеральный закон «О персональных данных» от 27 июля 2006 года №152-ФЗ.
- Постановление Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».
- Постановления Правительства Российской Федерации от 6 июля 2008 года №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».
- Письмо Рособразования от 3 сентября 2008 года №17-02-09/185 «О предоставлении уведомлений об обработке персональных данных».
- Постановление Правительства Российской Федерации от 15 сентября 2008 года №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
- Письмо Рособразования от 27 июля 2009 года №17-110 «Об обеспечении защиты персональных данных».

Полный перечень на сайте
http://77.rkn.gov.ru/law/p4735/

Ответственность за нарушение 152-ФЗ

- Административная: штаф или штраф с конфискацией несертифицированных средств обеспечения безопасности и шифровальных средств (Административный кодекс, ст. 13.11, 13.12, 13.14)
- Дисциплинарная: увольнение провинившегося работника (Трудовой кодекс РФ, ст. 81 и 90)
- Уголовная: от исправительных работ и лишения права занимать определенные должности до ареста (УК РФ, ст. 137, 140, 272)

Этапы организации защиты ПДн

- Инвентаризация ИСПДн
- Разграничение прав доступа работников к ПДн
- Документальное регламентирование работы с ПДн
- Формирование модели угроз безопасности ПДн
- Подготовка и отправка в уполномоченный орган (регулятору) уведомления об обработке ПДн
- Приведение системы защиты ПДн в соответствие с требованиями регуляторов
- Обеспечение надлежащего контроля безопасной эксплуатации ИСПДн

Инвентаризация ИСПДн

- Определение в ОУ существующих ИС и/или хранилищ данных, в которых осуществляется обработка ПДн
- Определение мест обработки ПДн для выявленных ИС и/или хранилищ данных
- На основе проведенной инвентаризации осуществляется разработка документов:
  - Список ИСПДн, в которых обрабатываются ПДн
  - Перечень сведений, составляющих ПДн
  - Перечень сотрудников, допущенных к обработке ПДн
  - Классификация ИСПДн
  - Разрешительная система доступа к ПДн
  - Концепция информационной безопасности
  - Политика информационной безопасности
  - Положение об обработке ПДн

Разграничение прав доступа работников к ПДн

- Ограничение физического доступа
- Ограничение электронного доступа:
  - Сотрудники, которым разрешено изменение
  - Сотрудники, которым разрешено чтение
  - Прочие сотрудники, которым доступ запрещен

Регламентирование работы с ПДн

- Разработка формы согласия на обработку ПДн
- Получение согласия на обработку ПДн
- Издание приказа о назначении лиц, ответственных за обработку ПДн
- Принятие положения о разграничении прав доступа к обрабатываемым ПДн
- Заключение соглашения о неразглашении информации с ответственными за обработку ПДн лицами
- Разработка и утверждение инструкций администратора ИСПДн, пользователя ИСПДн и администратора безопасности ИСПДн.

Формирование модели угроз безопасности ПДн

Разрабатывается на основании утвержденных Федеральной службой по техническому и экспортному контролю (ФСТЭК) документов:

- Базовая модель угроз безопасности ПДн при их обработке в ИСПДн
- Методика определения актуальных угроз безопасности ПДн при их обработке в ИСПДн

Уведомление об обработке ПДн

Осуществляется посредством заполнения формы на сайте:
http://pd.rkn.gov.ru/operators-registry/notification/form/
в электронном виде либо бумажном носителе с подписью уполномоченного лица

Соответствие системы защиты требованиям регуляторов

Оператор (т.е. ОУ) обязан обеспечивать безопасную обработку (в том числе и хранение) ПДн. Отсюда вытекает необходимость:

- Определения и обеспечения технических средств защиты ПДн
- Выполнения регламентированных резервирования и восстановления данных ИСПДн

В качестве оценки соответствия ИСПДн 1 и 2 классов требованиям к безопасности ПДн используется обязательная сертификация (аттестация)

Обеспечение надлежащего контроля безопасной эксплуатации ИСПДн

Мероприятия по контролю за соблюдением регламентов по работе с ПДн:

- Учет инцидентов – обращений субъектов ПДн о выполнении их законных прав
- План внутренних мероприятий по контролю и нарушению при обработке ПДн, журнал проведенных проверок и принятых мер
- Разработать и осуществить процедуру резервного копирования и восстановления данных

Порядок действий перед проверкой Роскомнадзора

- Ваше ОУ в реестре операторов персональных данных ?
  http://pd.rkn.gov.ru/operators-registry/operators-list
- Через специальную форму http://www.rsoc.ru/personal-data/forms/p333/ внести необходимые изменения
- Подготовить, издать и утвердить пакет документов, соблюдая формулировки законодательных актов
  - ответственный за организацию обработки персональных данных
  - администратор безопасности персональных данных
  - закрепить на бумаге места хранения и ответственных за сохранность ПДн в кабинетах
  - назначить комиссию по классификации и комиссию по уничтожению ПДн

Действия перед проверкой Роскомнадзора (продолжение)

- определить лица, допущенные к обработке ПДн сотрудников, контрагентов, учеников, родителей...
  - какой работник к каким данным имеет доступ
  - какой тип обработки ПДн используется
  - какова роль работника в системе при автоматизированной обработке
  - соглашение о неразглашении ПДн
- определить категории ПДн, подлежащих защите
- утвердить перечень сведений конфиденциального характера (ПДн входят в такой перечень), выбирая пункты из указа президента РФ № 188 от 6 марта 1997 г.
- разработать и утвердить основной документ – Положение об обработке и защите ПДн

Действия перед проверкой Роскомнадзора (продолжение)

- Разработать и регулярно заполнять:
  - Журнал проведения инструктажа по информационной безопасности
  - Журнал учета мероприятий по контролю обеспечения защиты персональных данных
  - Журнал учета обращений граждан-субъектов персональных данных о выполнении их законных прав
- Вспомнить про журнал учета проверок юридических лиц контролирующими органами

Примерный перечень документов для проверки

- Концепция информационной безопасности.
- Приказ о создании СЗ ПДн.
- План мероприятий по обеспечению защиты ПДн.
- Отчет о результатах проведения внутренней проверки.
- Перечень сведений, составляющих ПДн.
- Список ИСПДн, в которых обрабатываются ПДн.
- Разрешительная система доступа к ПДн.
- Перечень сотрудников, допущенных к обработке ПДн.
- Перечень защищаемой информации.
- Положение по обработке персональных данных.
- Политика ИБ.
- Инструкция пользователя ИСПДн.
- Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций.
- Инструкция администратора ИБ ИСПДн.
- Инструкция по организации парольной защиты.

Примерный перечень документов для проверки (продолжение)

- Инструкция по антивирусной защите.
- Инструкция по обработке ПДн без использования средств автоматизации.
- Перечень ПДн с местами хранения, обработки и списком допущенных лиц.
- Приказ о введении в действие документов, регламентирующих мероприятия по защите ПДн.
- Приказ о создании комиссии по классификации ИСПДн.
- Приказ о создании комиссии по уничтожению ПДн.
- Журнал регистрации фактов несанкционированного доступа.
- Журнал учета обращений граждан-субъектов ПДн.
- Журнал учета пользователей ИСПДн, прошедших обучение правилам работы с СЗИ.
- Журнал учета мероприятий по контролю ИБ.
- План проверочных мероприятий по обеспечению безопасности ПДн.
- АКТ классификации ИСПДн.
- Приказ о назначении администратора ИБ.
- Согласие работника на обработку его ПДн.

Обеспечение защиты детей от информации, несовместимой с целями образования

- Централизованное и единое управление локальной сетью
- Сегментирование локальной сети на основе управляемых коммутаторов
- Организация адресного пространства и закрепление арендуемых адресов
- Использование безопасных DNS-серверов
- Исключение из фильтрации сотрудников с особым функционалом

Контент-фильтрация

- «Белые списки» в качестве ресурсов Интернет для учеников на ученических ПК и всех подключающихся по беспроводной сети
- Запрет доступа к ресурсам Интернет, включенным в «Черные списки» для сотрудников с типовым функционалом
- Обеспечение доступа к определенным ресурсам для отдельных групп пользователей и конкретных ПК
- Исключение из фильтрации сотрудников с особым функционалом
- Регулярная корректировка списков доступа в Интернет

Контроль доступа в Интернет

- Электронные журналы доступа к ресурсам Интернет
- Разграничение прав доступа по пользователям
- Аутентификация при доступе к ресурсам Интернет/локальной сети
- Исключение возможности неконтролируемого подключения к локальной сети, особенно к административному сегменту

Подавайте заявки электронной почтой

- abuse@tgl.net.ru – корректировка работы системы контентной фильтрации, базирующейся на прокси-сервере, обслуживаемом МАОУ ДПО ЦИТ
- infosafety@tgl.net.ru – обращения, относящиеся к сфере информационной безопасности в деятельности ОУ
- monitoring_ikt@tgl.net.ru – обращения, относящиеся к сфере информатизации ОУ
- schools@tgl.net.ru – техническое обслуживание и программное сопровождение (исключая корректировку работы системы контентной фильтрации)

Заполняйте поля заявки

- В поле «Тема:» следует кратко указать Заказчика услуги, наименование услуги и желаемый срок исполнения.
- В теле письма следует подробно описать требующую решения проблемную ситуацию, местонахождение и телефон для связи с заинтересованным лицом и возможный период для выполнения работ.
- Для пояснения проблемной ситуации возможно вложить в письмо файл в формате «txt», «png», «7z», «zip» размером до 1 МБ.

Обратная связь

- Внимательно читайте нормативные и регламентирующие документы, договоры и инструкции
- Задавайте правильные вопросы, подробно описывая ситуацию и поставленные задачи
- Будьте вежливы и корректны в выражениях

Центральный офис ЦИТ:
office@tgl.net.ru тел/факс 22-37-73
Автозаводский офис ЦИТ тел/факс 32-73-40

Вопросы ?

- ?
- ?
- ?

Спасибо за внимание