Казенное учреждение Омской области
«Региональный информационно-аналитический центр
системы образования»
www.obr55.ru

РИАЦ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В ОРГАНИЗАЦИЯХ СФЕРЫ ОБРАЗОВАНИЯ

КАК
защитить данные?

ЗАЧЕМ
следовать рекомендациям по защите информации?

ПОЧЕМУ
информационная безопасность — это важно?

Омск — 2021

ТОЛЬКО ФАКТЫ

- В 2020 году специалистами InfoWatch зафиксировано 404 утечки данных из коммерческих, некоммерческих (государственных, муниципальных) организаций в России.
- 79% утечек были спровоцированы внутренними нарушителями (сотрудниками организаций), 21% — внешними нарушителями.
- Резко выросла доля умышленных нарушений в России. Почти 80% всех утечек в 2020 году совершены преднамеренно. Это свидетельствует о возросшем спросе преступного мира на конфиденциальную информацию.
- Почти 20% утечек в России происходит через канал мгновенных сообщений (мессенджеры).
- Чаще всего утекают персональные данные — 86% всех утечек.

Экспертно-аналитический центр InfoWatch. «Россия: утечки информации ограниченного доступа, 2020 год» (www.infowatch.ru/www.infowatch.ru/analytics)

Утечки конфиденциальной информации по-прежнему оказывают огромное воздействие на местные органы власти и муниципальные организации. Они являются идеальной мишенью для киберпреступников, поскольку предоставляют гражданам услуги, задействующие целый спектр различной конфиденциальной информации. Кибератаки подрывают репутацию госучреждений и снижают уровень доверия к ним.

ПОЧЕМУ ИНФОРМАЦИЯ НУЖДАЕТСЯ В ЗАЩИТЕ?

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ — ЗАДАЧА ВСЕХ РАБОТНИКОВ

Состояние безопасности организации (как информационной, так и, например, пожарной) зависит от каждого.

В 2020 году в мире наиболее привлекательной для нарушителей оказалась сфера образования. В ней почти 83% зарегистрированных утечек оказались умышленного характера.

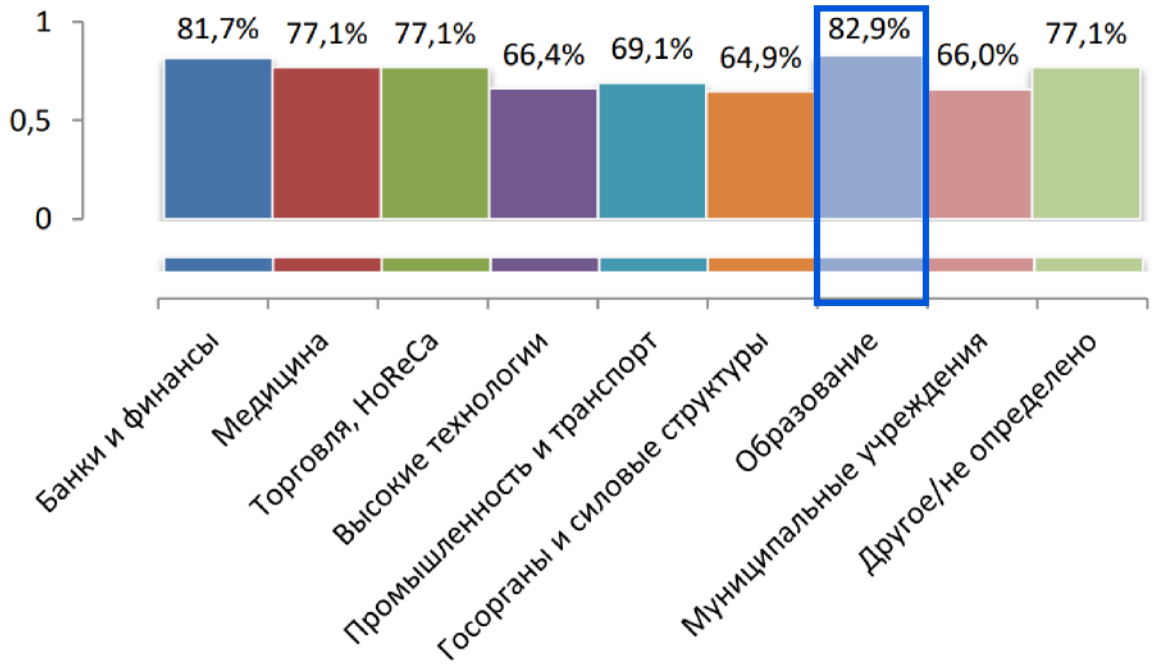


Рис. Доля умышленных утечек персональных данных от общего количества утечек персональных данных по отраслям, 2020г.

Экспертно-аналитический центр InfoWatch. «Исследование утечек информации ограниченного доступа в 2020 году» (www.infowatch.ru/analytics)

В целом, всплеск доли умышленных утечек отмечен во всех отраслях, что в первую очередь связано с существенным ростом ликвидности данных в период пандемии. В результате совокупная доля умышленных утечек составила 72,5%, тогда как годом ранее было 60,2%.

С ПОМОЩЬЮ ЧЕГО ПРОИСХОДЯТ УТЕЧКИ ИНФОРМАЦИИ?

В мире заметна тенденция к росту доли утечек, случившихся через Сеть: согласно последним данным, доля утечек по сетевому каналу в 2020 году составила более 79,3%. В 2018 году данный показатель составил 62,9%.

Доля утечек по электронной почте всё ещё остаётся на достаточно высоком уровне. Этот канал активно используется для фишинговых атак.

Более заметную роль в России стал играть канал мгновенных сообщений, связанный с передачей текстовых, голосовых и видео-сообщений (19,7%). Излюбленным средством для нарушителей стали мессенджеры.

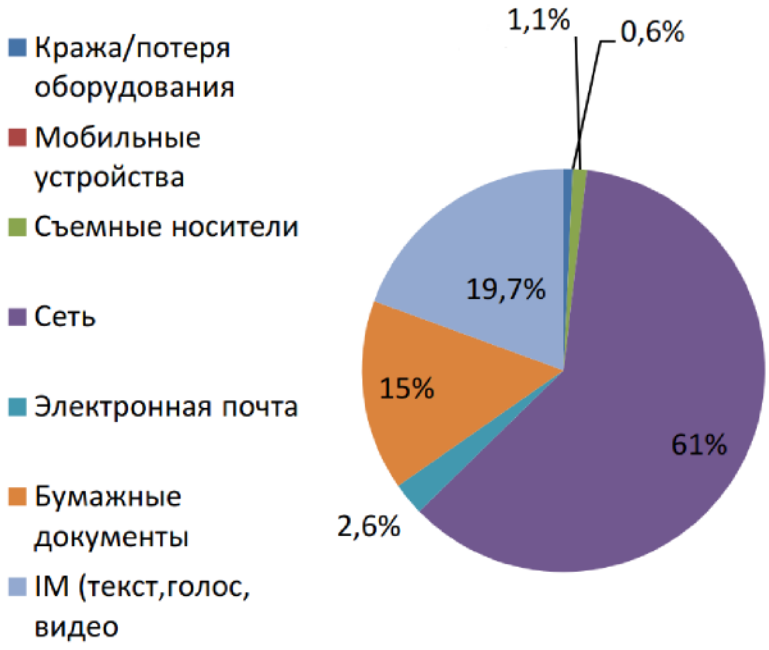


Рис. Распределение утечек по каналам, Россия, 2020г.

Экспертно-аналитический центр InfoWatch (www.infowatch.ru)

Проанализировав ситуацию за 3 последних года, можно заметить продолжение роста количества умышленных утечек, доли утечек персональных данных и коммерческой тайны, увеличение доли сетевого канала одновременно со снижением роли бумажных документов.

АТАКИ НА ОБРАЗОВАНИЕ

В первые пять месяцев 2020 года резко вырос интерес хакеров к образовательным ресурсам (электронные дневники, площадки онлайн-уроков и т.п.)

Также наблюдалось значительное увеличение количества атак на государственные учреждения.

Ростелеком-Солар. «DDoS-атаки в период COVID-19» (www.rt-solar.ru/analytics/reports)

ПРИМЕРЫ РЕАЛИЗОВАНЫХ АТАК НА ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ

21 сентября 2020 года непрерывной распределённой сетевой атаке подверглась государственная информационная система «Образование» Вологодской области. Система, состоящая из трёх подсистем *«Электронная школа», «Электронный детский сад» и «Электронный колледж»*, была недоступна в течение нескольких дней. Кроме того, перестали работать сайты образовательных организаций и почтовые сервисы системы образования. Благодаря тому, что хакерская атака была своевременно обнаружена, утечку данных удалось предотвратить.

Источник: Сайты вологодских школ и электронные дневники подверглись кибератаке (www.dp.ru/a/2020/09/24/Sajti_vologodskih_shkol_i)

Другая ситуация произошла в США. Выяснилось, что в 2021 году вымогательские группировки опубликовали данные, похищенные более чем у 1200 американских общеобразовательных школ. В файлах, похищенных хакерами у школ и опубликованных на сайтах утечек, обнаружили персональные данные детей.

В открытом доступе помимо ФИО школьников оказались, например, сведения о состоянии здоровья и экономическом положении семьи, а также другие типы данных, такие как номера социального страхования и даты рождения, являющиеся постоянными в течение всей жизни человека. Их утечка может иметь долгосрочные последствия и повлиять на ребенка, когда он уже вырастет.

Источник: Хакеры публикуют данные школьников: Родители бессильны (www.securitylab.ru/news/524363.php)

ОБЪЕКТЫ ЗАЩИТЫ

Основываясь на данных о реализованных угрозах, можно сделать вывод, что обеспечение безопасности информации ограниченного доступа — *современная необходимость.* Однако, в первую очередь, нужно определиться, что следует относить к объектам защиты.

К объектам защиты относятся:

- персональные данные (ПДн),
- средства криптографической защиты информации (СКЗИ) и их среда функционирования,
- парольная и аутентифицирующая информация, СКЗИ и носители (диски, флешки),
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация и материальные носители защищаемой информации, порядок доступа к ним,
- используемые информационной системой (ИС) каналы связи,
- помещения, в которых находятся ресурсы ИС и СКЗИ.

Регулирование отношений в сфере защиты персональных данных составляет 152-ФЗ «О персональных данных» и принятые в соответствии с ним иные нормативно-правовые акты.

КАКУЮ ИНФОРМАЦИЮ НУЖНО ЗАЩИЩАТЬ?

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Если совокупность данных необходима и достаточна для идентификации лица, такие данные следует считать персональными данными этого субъекта — ПДн (даже при отсутствии данных документа, удостоверяющего личность).

ПДн признается совокупность данных, прямо или косвенно с достаточной вероятностью указывающая на физическое лицо. Номер телефона и адрес электронной почты в совокупности с иными данными также отнесены к ПДн (ПП от 13.09.19 N 1197).

Пример: Набор [ФИО + страна проживания] не является ПДн, однако набор [ФИО + название населённого пункта с менее чем 1000 жителями] уже может быть достаточным для идентификации конкретного физического лица, а значит является ПДн.

Специальные категории ПДн касаются расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Биометрические ПДн характеризуют физиологические и биологические особенности человека, которые используются оператором для установления личности субъекта — фото на пропуске, если оно используется для сравнения фото с лицом предъявителя, дактилоскопические данные и др.

Лица, чьи данные обрабатываются (т. е. учащиеся, сотрудники организации и т.д.) — являются субъектами ПДн.

Таким образом, защита ПДн актуальна для любой организации, хотя бы по причине того, что в каждой организации обрабатываются ПДн сотрудников.

КТО ЗАНИМАЕТСЯ ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ?

Обработка персональных данных — любое действие или их совокупность, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Все эти действия могут совершаться с помощью средств автоматизации или без использования таковых.

Оператор персональных данных — государственный орган, муниципальный орган, юридическое или физ. лицо, самостоятельно или совместно с другими лицами осуществляющее обработку ПДн, а также определяющее цель и состав ПДн.

Если организация осуществляет только сбор персональных данных в другую организацию (является поставщиком ПДн), она также будет являться оператором, так как данное действие над ПДн (сбор) попадает под понятие обработки ПДн.

Таким образом, операторами ПДн в сфере образования являются:

- Министерство образования,
- муниципальные органы управления образованием,
- общеобразовательные организации,
- образовательные организации дошкольного и дополнительного образования,
- иные организации сферы образования.

СОГЛАСИЕ СУБЪЕКТА ПДН

В соответствии со ст. 9 закона «О персональных данных» от 27.07.2006 № 152-ФЗ субъект персональных данных самостоятельно принимает решение о предоставлении права на обработку и использование этой информации третьими лицами. Согласие оформляется в письменном виде или в электронном.

Одни и те же данные одного и того же человека могут обрабатываться в разных целях. И взятое в одном случае согласие — на другой случай может не распространяться.

Согласие должно содержать определенные сведения:

- ФИО и адрес субъекта ПДн,
- реквизиты документа, удостоверяющего личность,
- сведения об операторе,
- цель обработки ПДн,
- перечень обрабатываемых ПДн,
- перечень возможных действий с ПДн,
- сроки обработки ПДн и способ отзыва согласия,
- подпись субъекта ПДн.

Согласие на обработку ПДн должно учитывать возраст субъекта. Согласие несовершеннолетнего *(от 14 до 18 лет)* должно быть получено от самого несовершеннолетнего с согласия его законного представителя с указанием реквизитов документа, подтверждающего его полномочия (п. 1 ст. 26 Гражданского кодекса РФ).

Предоставление ПДн — действие, направленное на раскрытие ПДн определенному кругу лиц.
Распространение ПДн — действие, направленное на раскрытие ПДн неопределенному кругу лиц.
Для распространения ПДн (например, публикация в открытом доступе персональных данных на сайте школы) необходимо получить согласие от субъекта ПДн на распространение его ПДн. Это согласие оформляется отдельно от согласия на обработку ПДн.

Оператор может получить рекомендации Роскомнадзора по форме согласия на обработку ПДн, разрешенных для распространения:
www.pd.rkn.gov.ru/soglasiya/maket

ЗАПРОСЫ СУБЪЕКТОВ ПДН, ОТЗЫВ СОГЛАСИЯ

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн (подтверждение факта обработки, цель, способы обработки, местонахождение оператора, сроки обработки и т. д. – ч. 7 ст. 14 152-ФЗ).

В организации-операторе ПДн должен вестись Журнал учёта и регистрации обращений субъектов ПДн. Оператор обязан зарегистрировать запрос и предоставить данные субъекту.

Запросы субъектов ПДн могут содержать в себе требования: ознакомления, уточнения, блокирования, уничтожения ПДн, получения информации о способах, целях, сроках обработки ПДн и др. Предоставление сведений по запросу или мотивированный отказ предоставляется субъекту в течение 30 дней.

Субъект ПДн в любое время вправе отозвать согласие на обработку своих персональных данных (ч. 2 ст. 9 152-ФЗ). В подобной ситуации продолжение обработки персональных данных работника без его согласия возможно при наличии оснований, перечисленных в п. п. 2 - 11 ч. 1 ст. 6, ч. 2 ст. 10, ч. 2 ст. 11 152-ФЗ.

Человеку, который отказывается давать согласие, выдается форма, где разъяснены последствия отказа (например: без согласия не будет передана информация в организацию N). Возможен случай, когда человек, прочитав форму отказа с разъяснениями, подписывает согласие.

УВЕДОМЛЕНИЕ ОБ ОБРАБОТКЕ ПДН

Перед тем, как начать собирать ПДн, оператору необходимо направить уведомление об обработке ПДн в Роскомнадзор. Информация об операторе будет включена в реестр операторов.

Уведомление заполняется в электронной форме на сайте: www.pd.rkn.gov.ru/operators-registry/notification/form, а затем отправляется в бумажном виде.
Если произошли какие-то изменения в процессе обработки ПДн, оператору необходимо направить уведомление о внесении изменений в сведения в реестре операторов в течении 10 рабочих дней с момента возникновения изменений.
В случае прекращения обработки ПДн оператор в течении 10 рабочих дней сообщает об этом в Роскомнадзор.

Методические рекомендации утв. приказом Роскомнадзора N 94 от 30 мая 2017 г.

Сведения об операторе

Тип оператора * — Юридическое лицо

Наименование оператора *

Сокращенное наименование оператора:

Адрес оператора *

Индекс

Адрес местонахождения [выбрать]

☐ совпадает с адресом местонахождения

Индекс

Почтовый адрес [выбрать]

Рис. Начало формы уведомления

ОБРАБОТКА ПДН БЕЗ СРЕДСТВ АВТОМАТИЗАЦИИ

Обработка ПДн бывает трёх видов:

- Неавтоматизированная обработка — это обработка ПДн на бумажных носителях.
- Автоматизированная обработка (или обработка в информационных системах ПДн) предполагает использование средств автоматизации.
- Смешанная обработка включает автоматизированную и неавтоматизированную обработку ПДн. Она встречается наиболее часто.

Обработка персональных данных считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия осуществляются при непосредственном участии человека.

Защита персональных данных при неавтоматизированной обработке осуществляется в соответствии с Постановлением Правительства РФ от 15 сентября 2008 г. N 687.

Правила обработки ПДн без средств автоматизации:

- раздельное хранение ПДн, имеющих разные цели обработки,
- определение надежных мест хранения ПДн,
- доступ к ПДн имеет ограниченный круг лиц,
- согласие субъекта ПДн на обработку его ПДн без средств автоматизации.

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ?

Информационная система персональных данных (ИСПДн) — это совокупность ПДн (базы данных) и обеспечивающих их обработку информационных технологий и технических средств.

Возможные ИСПДн в организации сферы образования:

- ИСПДн «Зарплата и кадры»,
- ИСПДн «Обучающиеся»,
- ГИС «РИС ГИА»,
- АИС «Зачисление в ОО»,
- ИСПДн «Дневник.ру»,
- ИСПДн «Дополнительное образование»,
- ИСПДн «АРМ ФИС ФРДО»,
- ГИС ДДО (ранее — АИС «Комплектование ДОО»),
- и другие.

Понятие ИСПДн включает в себя не только информацию о субъектах ПДн. Её компонентами также являются технические средства, информация и ее носители, процессы обработки и передачи информации и т.п.

Например, в ИСПДн АИС «Зачисление в ОО» в школе входят:

- сами ПДн (ФИО, адрес, класс, сведения о льготах и т.д.)
- компьютер, за которым работает сотрудник школы,
- программы, с помощью которых обрабатываются ПДн (браузер, Word и др.),
- защитные программы (антивирус и др.)

ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАНИИ

МЕРЫ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, утечки, уничтожения, изменения и др.
Обеспечение безопасности ПДн достигается, в частности:

- определением угроз безопасности ПДн,
- применением организационных и технических мер по обеспечению безопасности ПДн в соответствии с уровнем защищенности ПДн,
- применением сертифицированных средств защиты информации,
- оценкой эффективности принимаемых мер по обеспечению безопасности ПДн,
- учетом машинных носителей ПДн,
- обнаружением фактов несанкционированного доступа к ПДн, предупреждением и ликвидацией последствий компьютерных атак, восстановлением ПДн,
- установлением правил доступа к ПДн,
- контролем за принимаемыми мерами и уровнем защищенности ПДн,
- периодический внутренний контроль соответствия принятых мер по защите информации.

ст. 18.1, ст. 19 ФЗ от 27 июля 2006 г. N 152-ФЗ «О персональных данных»

Состав мер для защиты информации выбирается с учетом актуальных угроз, уровня защищенности ПДн, применяемых информационных технологий. Основной перечень программно-технических средств защиты информации в ИСПДн:

- средства защиты информации от несанкционированного доступа (Dallas Lock, Secret Net и т.д.),
- средства криптографической защиты информации (КриптоПро CSP, VipNet Client и т.д.),
- средства антивирусной защиты (Dr.Web, Kaspersky Anti-Virus и т.д.),
- межсетевой экран (VipNet Coordinator HW и т.д.)

СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Средство криптографической защиты информации (СКЗИ) — средства шифрования, электронной подписи, средства изготовления ключевых документов, ключевые документы, аппаратные и программно-аппаратные шифровальные (криптографические) средства.

Примеры СКЗИ:

- электронная подпись,
- токен члена ГЭК,
- КриптоПро CSP, VipNet CSP, Код безопасности CSP,
- криптомаршрутизатор и т.д.

Правила пользования СКЗИ:

- СКЗИ выдается под расписку в Журнале учета СКЗИ,
- пользователь несет персональную ответственность за полученные СКЗИ,
- необходимо своевременно обновлять операционную систему, программные средства, антивирусные базы,
- использовать надежные пароли,
- запрещено пересылать электронные подписи по электронной почте, передавать третьим лицам, копировать на компьютер,
- не оставлять носитель с электронной подписью в компьютере, на столе без присмотра,
- носитель с электронной подписью должен храниться в опечатываемом сейфе, закрывающемся ящике в контролируемой зоне,
- после увольнения сотрудника, его электронная подпись должна быть аннулирована,
- пользователь оповещает ответственного за защиту информации об утере, компрометации СКЗИ,
- СКЗИ с истекшим сроком действия необходимо уничтожить,
- помещения, в которых находятся СКЗИ, являются спецпомещениями, поэтому к ним должен быть ограничен несанкционированный доступ.

Приказ ФАПСИ от 13.06.2001 N 152

КОНТРОЛИРУЕМАЯ ЗОНА

Для ИСПДн приказом должны быть утверждены кабинеты, помещения, в пределах которых осуществляется обработка ПДн и/или располагаются средства криптографической защиты информации — контролируемая зона (КЗ). В пределах КЗ (кабинеты по периметру) должен осуществляться контроль за пребыванием и действиями лиц.

Кроме того, утверждается схема расположения технических средств, находящихся в пределах КЗ. После её утверждения не рекомендуется менять места расположения технических средств и запрещается их вынос за границы КЗ.

Пребывание посторонних лиц в границах КЗ возможно только в присутствии ответственных пользователей.

Требования о назначении контролируемой зоны и регулирующие доступ в помещения с ПДн и СКЗИ приводятся в следующих нормативных правовых документах:

- Приказ ФСБ России от 10.07.2014 N 378,
- Приказ ФАПСИ от 13.06.2001 N 152,
- Постановление Правительства от 01.11.2012 N 1119.

В организации-операторе ПДн должен соблюдаться ряд требований по доступу в помещения, в которых ведётся обработка ПДн и/или хранятся СКЗИ:

- должен быть утвержден перечень лиц, имеющих доступ в помещения,
- должен быть утвержден перечень лиц, имеющих допуск к обработке ПДн,
- должна быть утверждена и соблюдаться процедура опечатывания помещений в конце рабочего дня последним покидающим кабинет работником,
- все факты выдачи и сдачи ключей от помещений должны быть зафиксированы соответствующими записями в Журнале учета выдачи ключей от кабинетов,
- сотрудники организации-оператора ПДн обязаны информировать руководство о признаках несанкционированного прохода в помещения контролируемой зоны.

ПЕРЕДАЧА ПДН

Передача персональных данных по каналам связи, не защищенным от перехвата нарушителем (например, по сети Интернет или при выносе ПДн за пределы контролируемой зоны) возможна:

- по сети Интернет с использованием СКЗИ (например, подключение и передача данных в зашифрованном виде с помощью Континент TLS-клиент, КриптоПро CSP, VipNet Client и т.д.),
- передача зашифрованных файлов на съемном носителе (например, на USB-флеш-накопителе),
- передача документов на бумажных носителях.

Таким образом, категорически запрещено отправлять ПДн по электронной почте, через мессенджеры (например, WhatsApp), социальные сети, облако (например, Яндекс.Диск, Облако Mail.ru), сканировать документы с ПДн с последующей их отправкой по незащищенным каналам связи (например, по электронной почте).

- Приказ ФСБ России от 10 июля 2014 г. N 378,
- Приказ ФСТЭК от 18 февраля 2013 г. N 21,
- ст. 19 ФЗ от 27 июля 2006 г. N 152-ФЗ «О персональных данных»,
- Методические рекомендации утв. ФСБ России 31 марта 2015 г. N 149/7/2/6-432.

По отношению к электронным носителям с ПДн выдвигаются следующие требования:

- в Журнале учета машинных носителей персональных данных должен вестись учет носителей, хранящих ПДн и участвующих в их обработке: жесткие диски (в корпусе ПК), внешние жесткие диски, USB-флеш-накопители,
- съемные носители (внешние жесткие диски, USB-флеш-накопители) должны храниться в опечатываемых сейфах или тубусах с пломбой в контролируемой зоне.

ПОЛИТИКА ЧИСТОГО СТОЛА/ЭКРАНА

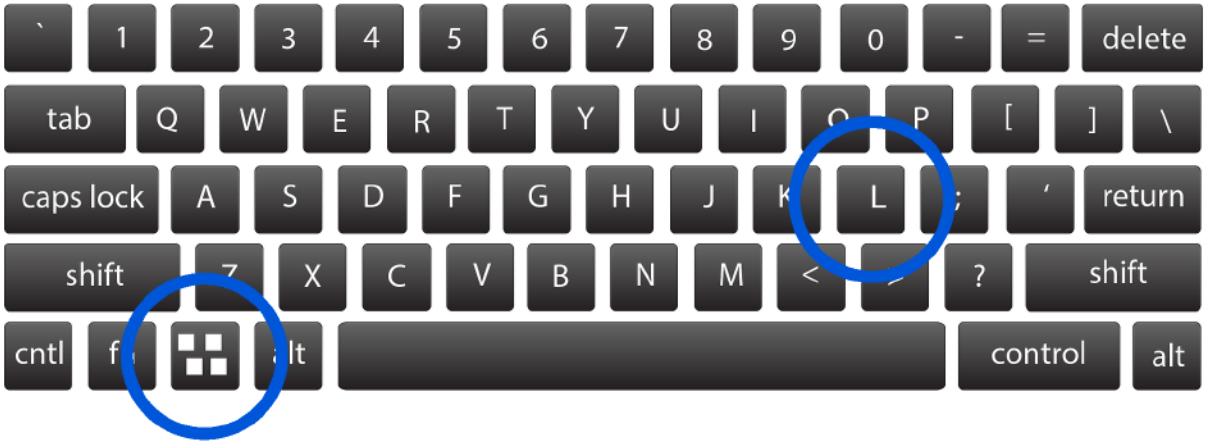
Еще одной важной мерой защиты информации в ИСПДн является соблюдение политики «чистого стола».

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители паролей и хранения их вблизи рабочих мест.

При работе с защищаемой информацией следуйте следующим правилам:

- расположите монитор, исключив его несанкционированный просмотр третьими лицами: закройте окна жалюзи, отверните монитор от окон и дверей,
- не храните стикеры с паролями на видном и в легкодоступном месте,
- не оставляйте печатные документы открытыми на столе, в принтере,
- все хранящиеся документы должны быть подшиты в папки и убраны в шкаф в конце рабочего дня,
- ненужные документы необходимо измельчать,
- если USB-накопители, жесткие диски с персональными данными больше не используются, то необходимо гарантированно уничтожить содержащуюся на них информацию перед тем, как выбросить,
- покидая рабочее место, блокируйте учетную запись и прячьте носители в недоступное для посторонних место.

Блокировка учётной записи производится комбинацией клавиш Windows + L



ИСПОЛЬЗУЙТЕ ПАРОЛЬНЫЕ ФРАЗЫ

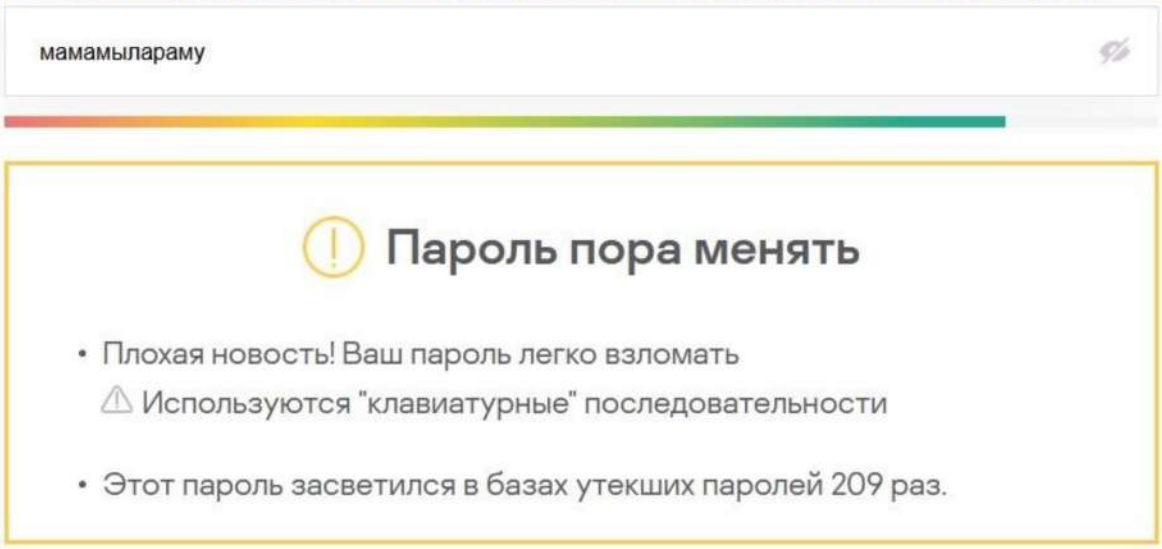
В ИСПДн должна соблюдаться политика паролей. Для электронной почты, для входа в операционную систему, для авторизации на сайте используются надежные пароли. Сложные пароли позволяют повысить уровень безопасности и сохранности данных. Но в то же время, сохранность самих паролей — также важный вопрос.

Пароль Fnw{fi2%dMk#mw$s является надежным, но его сложно запомнить и сложно вводить при каждом входе, поэтому рекомендуется использовать парольные фразы (например, ДеловойСкорпионПоблагодарилКреветку). Их легко запоминать и вводить, не нужно записывать, а из-за своей длины они считаются более безопасными.

При назначении нового пароля следуйте правилам:

- используйте парольные фразы длиной минимум 8 символов,
- для разных аккаунтов используйте разные пароли,
- будьте оригинальны (не указывайте в качестве пароля ФИО, имена родственников и т. д., не используйте очевидные фразы, устойчивые выражения),
- использование цифр и специальных символов (!@#%) ещё больше увеличивает надёжность вашего пароля,
- периодически производите смену паролей,
- для хранения паролей подходят менеджеры паролей,
- для генерации парольных фраз можно использовать генераторы (например, VipNet Password Generator: www.infotecs.ru/product/vipnet-password-generator.html).

Проверьте надежность своего пароля: https://password.kaspersky.com/ru



ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Из-за возможных негативных последствий от использования несертифицированного, нелицензионного программного обеспечения (ПО) существуют некоторые запреты. Простая программа, загруженная из интернета, может содержать в себе вирусы и обладать недекларированными возможностями, что может нанести большой вред как отдельному компьютеру, так и всей инфраструктуре организации-оператора ПДн.

К возникновению дополнительных угроз также ведут:

- хранение данных в облаке,
- удаленный доступ,
- использование сетей wi-fi с рабочих мест,
- использование нелицензионного ПО.

Для ИСПДн должен быть утвержден перечень разрешенного программного обеспечения. В перечень включается минимальный необходимый для работы набор программ. На рабочих местах ИСПДн может быть установлено ПО только из этого перечня и только из доверенных источников (с официального сайта, с установочного диска).

Важно своевременно устанавливать обновления используемых программ. С помощью обновлений разработчики устраняют уязвимости ПО. Чем больше проходит времени, тем больше находится «пробелов» в безопасности приложений, которыми могут воспользоваться злоумышленники.

Для автоматизированного обнаружения уязвимостей программного и системного обеспечения можно воспользоваться программой ScanOVAL, разработанной ФСТЭК: www.bdu.fstec.ru/site/scanoval

КОНТРОЛЬ И НАДЗОР

Контроль за обработкой ПДн в ИСПДн осуществляется сразу несколькими государственными ведомствами.

Роскомнадзор (РКН) контролирует обработку ПДн в соответствии с требованиями законодательства. До начала обработки ПДн оператор обязан направить уведомление в отделение РКН. Оператор также обязан в течении месяца уведомлять РКН об изменениях в используемых системах.

Федеральная служба по техническому и экспортному контролю РФ (ФСТЭК России) регулирует вопросы, связанные с технической защитой информации, средствами вычислительной обработки ПДн, за исключением криптографических средств, обновляет базу угроз безопасности и уязвимостей. Разрабатывает и устанавливает требования по обеспечению безопасности информации.

Федеральная служба безопасности России (ФСБ). Контролирующая функция ФСБ связана с СКЗИ, доступом в помещения, передачей конфиденциальных данных по защищенным каналам связи. Кроме того, ФСБ наделена полномочиями по контролю за выполнением организационных и технических мер по обеспечению безопасности ПДн при их обработке в информационных системах.

КТО ОСУЩЕСТВЛЯЕТ КОНТРОЛЬ ЗА ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ?

ОТВЕТСТВЕННОСТЬ

Ответственность за обработку ПДн возлагается как на юридические лица, так и на должностные лица. Нарушение требований законодательства в части обработки ПДн влечёт за собой компенсацию морального вреда, а также административную или уголовную ответственность.

Вид нарушения	Размер штрафа
Обработка ПДн без письменного согласия субъекта, либо обработка данных с нарушением требований к составу сведений, включаемых в такое согласие	Должностное лицо: 10-20 тыс. руб. Юр. лицо: 15-75 тыс. руб.
Невыполнение обязанности по опубликованию политики обработки ПДн	Должностное лицо: 3-6 тыс. руб. Юр. лицо: 15-30 тыс. руб.
Невыполнение требований об уточнении ПДн, блокировании, уничтожении (для устаревших, неточных данных и данных, полученных незаконно)	Должностное лицо: 4-10 тыс. руб., Юр. лицо: 25-45 тыс. руб.
Нарушение сохранности ПДн при хранении материальных носителей, несанкционированный доступ к ним	Должностное лицо: 4-10 тыс. руб., Юр. лицо: 25-50 тыс. руб.
Несоблюдение требований к обезличиванию ПДн	3-6 тыс. руб.
Нарушение требований по хранению ПДн на территории РФ	до 18 млн руб.

Уголовная ответственность:

- Незаконное собирание и распространение сведений о частной жизни (в т.ч. персональных данных):
  - штрафы 100-350 тыс. руб.
  - лишение права занимать должности до 5 лет
  - принудительные работы, арест
  - лишение свободы до 5 лет
- Отказ в предоставлении гражданину информации:
  - штрафы до 200 тыс. руб.
  - лишение права занимать должности на 2-5 лет

Источники:
ст. 5.39, ст. 13.11, ст. 19.7 КоАП РФ; ст. 137, 140 УК РФ

ПОДВЕДЁМ ИТОГИ

Выделим несколько основных тезисов:

- обеспечение информационной безопасности зависит от каждого сотрудника,
- организации сферы образования являются операторами персональных данных (ПДн),
- оператору необходимо актуализировать сведения в реестре операторов,
- организации сферы образования являются операторами информационных систем персональных данных (ИСПДн),
- оператор ПДн должен принимать организационные и технические меры меры по защите данных в ИСПДн,
- в ИСПДн необходимо использовать лицензионное программное обеспечение, установленное из надежных источников, сертифицированные средства защиты,
- запрещено передавать незашифрованные ПДн по сети (через мессенджеры, электронную почту, облако, соц. сети),
- оператор ИСПДн и сотрудники организации несут ответственность за нарушение законодательства в области ПДн.

Таким образом, защита информации должна осуществляться комплексно, сразу по нескольким направлениям. Чем больше методов будет задействовано, тем меньше вероятность возникновения угроз и утечки данных из информационных систем.