Личная безопасность учащихся в цифровой образовательной среде

А.Н. Рассказова[1], А.С. Зыкова[2].

[1] Северо-Западный государственный медицинский университет им. И.И. Мечникова,
[2] Севастопольский государственный университет

an_rasskazova@mail.ru, vesta.bereginya@gmail.com

Аннотация

Мы, как преподаватели, наделены правом и доступом к ежедневному сбору и обработке данные обучающихся. При этом наряду с освоением новых цифровых технологий сбора и обработки данных важно соблюдать их конфиденциальность и обязанность по защите. Несмотря на то, что защита конфиденциальности данных учащихся является частью основной ответственности за заботу о них, не во всех учебных заведениях имеются письменные договоренности и/или руководства по защите данных, а также какие-либо положения в отношении сбора и использования частной информации.

Таким образом, цель данной работы состоит в предложении рекомендаций по разработке политики конфиденциальности непосредственно в учебных заведениях. Для этого анализируется роль преподавателя в защите данных обучающихся с точки зрения осознанного управления информацией и обсуждается ряд мер по защите конфиденциальности данных учащихся, не нарушая образовательных целей и стиля работы преподавателя. Предметом анализа являются учащиеся системы общего образования, студенты средних специальных и высших учебных заведений.

Ключевые слова: персональные данные, доступа, контроль, прозрачность, ограничение использования, цифровые образовательные ресурсы

Библиографическая ссылка: Рассказова А.Н., Зыкова А.С. Личная безопасность в цифровой образовательной среде // Информационное общество: образование, наука, культура и технологии будущего. Выпуск 5 (Труды XXIV Международной объединенной научной конференции «Интернет и современное общество», IMS-2021, Санкт-Петербург, 24 – 26 июня 2021 г. Сборник научных статей). — СПб.: Университет ИТМО, 2021. С. 85-94. DOI: 10.17586/2587-8557-2021-5-85-94

1. Введение

На сегодняшний день условия преподавания меняются: обновляются федеральные государственные образовательные стандарты, профессиональные стандарты, а также оценка квалификации педагогов. Нововведения касаются не только традиционной организации занятия на базе существующих педагогических практик, но и организации в цифровой образовательной среде, в которой преподаватели, используя разные форматы обучения, ежедневно взаимодействуют с персональной информацией учащихся. Будь то организация определенного формата занятия, проведение экзамена или опроса, аудио или видеозапись собственных занятий – все эти действия так или иначе сопровождаются управлением личной информацией учащихся. Тем самым, с одной стороны, развитие цифровой образовательной среды диктует новые возможности сбора и обработки персональных данных учащихся. С другой – появляется риск утечки этих данных. Необходимость решения вопроса неразглашения персональных данных и обеспечения

личной безопасности учащихся в цифровой образовательной среде определяет актуальность темы настоящего исследования.

Цель данной работы состоит в предложении рекомендаций по обеспечению личной безопасности в цифровой образовательной среде. Предметом анализа являются следующие категории обучающихся: учащиеся системы общего образования, студенты средних специальных и высших учебных заведений. Для достижения цели сначала проанализируем прямые и косвенные факторы идентификации личности, а также дадим характеристику основных принципов конфиденциальности. Затем, принимая во внимание условия обеспечения конфиденциальности в цифровой образовательной среде, предложим искомые рекомендации.

2. Конфиденциальность личной информации

В настоящее время в области исследования конфиденциальности личной информации наблюдается следующее противоречие. С одной стороны, в качестве основной причины «утечки» персональных данных российские эксперты называют действия самих сотрудников компаний [1]. С другой стороны, сохранение конфиденциальности личной информации воспринимается компаниями одной из важнейших задач для сохранения доверия потребителей. Сегодня эта точка зрения достаточно активно обсуждается в специализированных интернет-сообществах. Действительно, факт того, что «приблизительно 60% потребителей не станут больше иметь дело с компанией, если узнают, что была похищена их собственная конфиденциальная информация" [2], мотивирует компании серьезно отнестись к управлению этого риска. Так в работе [3] обсуждаются меры предосторожности самих потребителей по защите личной информации. Однако указанные исследования не охватывают область образования. При этом риск, связанный с утерей или предоставлением данных в интернете со стороны молодого населения России (школьников 11-16 лет), все больше возрастает и несет в себе все большие негативные последствия [4]. Одним из них можно назвать рост объема затрат на выявление «утечки» данных. Так, например, согласно расчету стоимости утечки данных, выполненному в рамках исследовательского отчета Института Понемона (США) [5], средняя стоимость взлома данных из расчета на одну скомпрометированную запись в 2018 году составила 148 долларов. При этом, организациям требовалось в среднем 196 дней, чтобы обнаружить «утечку» данных. Кроме того, констатирован факт, что общая стоимость на душу населения и средний размер утечки данных (по количеству потерянных или украденных записей) увеличивается из года в год только в США.

Таким образом, вопрос обеспечения конфиденциальности личной информации является не только актуальным, но и малоизученным.

2.1. Прямые и косвенные факторы идентификации

Для придания информации статуса конфиденциальной в российском законодательстве рекомендовано использовать режим «охраняемой законом тайны». В Трудовом Кодексе РФ [6, п. 6, ч. 1 ст. 81] к ней относят государственную, банковскую, налоговую, служебную и «иную охраняемую законом тайну». В этом контексте для образовательных учреждений прежде всего актуальны персональные данные сотрудников и учащихся, а с учетом развития цифровой образовательной среды и организации на их базе онлайн-обучения – персональная информация пользователей, а также статистическая и аналитическая информация.

Наиболее очевидные пункты перечня персональных данных физических лиц, в том числе и учащихся образовательных учреждений, включают фамилию, имя отчество; пол, возраст; номер телефона; адрес проживания; адрес электронной почты, и другую контактную информацию. Что касается персональной информации в цифровой образовательной среде, например, пользователей онлайн-курсов, этот перечень может быть

расширен за счет добавления разного толка подлежащей обработке статистической и аналитической информации, а также информации, содержащейся в резервных и сетевых хранилищах. Все это информация, которую по умолчанию нельзя разглашать получившими к ним доступ лицами. Таким образом, при наличии подписанных соглашений о неразглашении информации или без них сотрудники соблюдают требования обеспечения невозможности идентификации личности третьими лицами.

Однако персональная информация может представлять собой ряд различных элементов данных, которые сами по себе не идентифицируют никого, но в сочетании с другой информацией позволяют понять, кто именно является индивидуумом. Например, если кто-то упоминает студента высокого роста, то, скорее всего, трудно понять, о ком идет речь без дополнительной информации. Невысокого роста студента также невозможно идентифицировать без специальных пояснений. При этом, описание учащегося типа «это тот, который высокого роста, в 10-м классе, высказавшийся вчера на пятом уроке по поводу культуры поведения в школе», поможет легко идентифицировать конкретного человека. Все это свидетельство того, что мы должны относиться к такого рода косвенно-идентифицирующей информации так же, как если бы это было имя человека, адрес электронной почты или другой прямой идентификатор индивидуума. Отсюда, возникает потребность под персональной информацией рассматривать не только прямые, но и косвенные факторы идентификации личности.

Развитие цифровой образовательной среды сопровождается внедрением в практику технологий отслеживания пользователей интернет-приложений (далее приложений). Данные технологии отслеживания позволяют поставщикам ресурсов собирать информацию, полезную для оценки производительности приложения, устранения неполадок и его улучшения. Такие технологии могут включать в себя информацию о количестве пользователей приложения, о том, сколько времени пользователи тратят на использование приложения, какие области приложения используются чаще всего, в каком порядке пользователи переходят к различным функциям приложения, а также какие функции приложения оказались не задействованными, как ожидалось.

Для случая с обучающимися индивидуумами такая технология может отслеживать частоту нажатия клавиш, например при онлайн-опросе, отвечая на следующие вопросы:

— сколько времени требуется учащемуся для формулирования ответа;
— сколько правильных и неправильных ответов записал студент;
— на какие типы вопросов был дан правильный ответ, а какие типы вызывают затруднения у студента с правильны ответом;
— насколько строгими могут быть вопросы, чтобы учащийся мог справиться с работой.

Такого типа данные называются статистическими в контексте их сбора и аналитическими – в контексте их обработки. При этом часть такого отслеживания проводится для того, чтобы убедиться, что приложение работает надлежащим образом, другая часть - для внутренних целей поставщика ресурсов, а третья часть - для целей обучения. Конечно, ответы на некоторые вопросы могут служить одновременно многим целям. Отсюда, следует вывод, что сортировка разного типа данных должна являться частью задачи определения того, какая информация считается личной информацией, требующей защиты, какие практики являются легитимными, например, в школьных условиях, и какая информация и методы ее использования могут поставить под угрозу конфиденциальность наших учеников.

Таким образом, когда речь идет о конфиденциальности данных учащихся, мы заботимся о защите их личной информации, которая может принимать многие из описанных выше форм. Это может быть прямой идентификатор, который легко распознать как личный, или это может быть комбинация косвенных идентификаторов. При этом мы можем быть осведомлены, например, после прочтения политики конфиденциальности, что мы или наши студенты предоставляют личную информацию по просьбе организатора конференции и/или поставщика ресурсов. Тем не менее независимо от способа сбора (онлайн-опроса или

непосредственно на офлайн-занятии и т.д.) или формы сбора (прямой или косвенной), такая персональная информация должна подлежать защите.

2.2. Основные принципы конфиденциальности

Несмотря на то, что данная работа не предполагает детального анализа законодательства в области защиты персональных данных, все же важно понять общий контур, в рамках которого укладываются основные требования к эффективной защите данных учащихся. Без этого трудно представить, какие данные наших учащихся нужно отнести к конфиденциальным в контексте того или иного формата обучения и какие решения следует принимать об их защите. Анализ имеющегося законодательства в области конфиденциальности и защиты данных позволяет более конструктивно сотрудничать с руководством учебного заведения по вопросу защиты данных обучающихся, удерживая процесс преподавания на высоком уровне.

Итак, мы уже затронули вопрос: «Что относится к конфиденциальной информации?» Федеральный закон "О коммерческой тайне" [7] является основным документом, определяющим информацию, которая относится к конфиденциальной. Использование коммерческой конфиденциальной информации позволяет ее обладателю получать коммерческую выгоду. Вместе с тем приведенный в этом законе перечень неполон и дополнен другими нормативными правовыми актами, где раскрыты понятия профессиональной тайны, такой как банковской, адвокатской, нотариальной тайны, тайны страхования, а также сведения, связанные с аудитом организации [8]. Однако понятия коммерческой тайны и конфиденциальной информации не тождественны. Коммерческая тайна также как и служебная тайна – это один из видов конфиденциальной информации [9], которая требует защиты.

Нас интересует конфиденциальная информация обучающихся системы общего образования, студентов средних специальных и высших учебных заведений в цифровой образовательной среде. Принимая во внимание это условие, распределим существующие российские законы конфиденциальности в соответствие с принципами надлежащей (справедливой) информационной практики (FIPPs – Fair Information Practice Principles) [10].

Принципы FIPP касаются сбора и использования личной информации, качества, безопасности, а также прозрачности данных. Выделяют несколько ключевых принципов для защиты требований к автоматизированным системам персональных данных. Первый принцип – это **прозрачность**, которая обеспечивается путем уведомления физических лиц о том, что сбор персональной информации не предполагает ее распространения без согласия субъекта персональных данных. ФЗ «О персональных данных» [11] обеспечивает соблюдение данного принципа, а ответственность за несоблюдение регламентирована в Кодексе РФ об административных правонарушениях [12, ст. 13.11].

Второй принцип – **обеспечение доступа** отдельных лиц для просмотра, копирования, корректировки или изменения личной информации учащегося с согласия или ведома самого учащегося или его родителя/опекуна. Соблюдение этого принципа регламентируется законом ФЗ «О персональных данных» [11, ст. 14], в соответствии с которым, прежде чем собирать личную информацию от кого-либо, мы должны сначала запросить и получить разрешение этого человека. В случае учащегося, не достигшего восемнадцатилетнего возраста или еще не поступившего в высшее учебное заведение, такое разрешение выдается родителем или законным опекуном.

Третий принцип – **ограничение использования** персональной информации с учетом цели по ее сбору. Для каждого элемента собранной информации существует конкретная причина ее получения и предполагаемое использование. Поэтому данный принцип определяет необходимость использования личной информации только для определенной цели, для которой она была собрана, и формулирования полномочий по ее сбору. Для этого в учебных заведениях должна использоваться политика конфиденциальности,

в соответствии с которой учащийся или его родитель предоставляет учебному заведению специальное разрешение. В случае, если речь идет о персональных данных студента, получающего образование в цифровой образовательной среде, то в рамках договора с разработчиком или с сопровождающим курса следует использовать «Соглашение о неразглашении информации» со стороны поставщика ресурсов с учетом целей, для которой собирается информация.

Четвертый принцип – **безопасность**. Безопасность данных имеет решающее значение для защиты личной информации от несанкционированного доступа. Личная информация не должна собираться, если она не может быть должным образом защищена. Соблюдение принципа безопасности предполагает защиту личной информации с помощью соответствующих стандартов безопасности от таких рисков, как потеря, несанкционированный доступ или использование, уничтожение, изменение или непреднамеренное/ненадлежащее раскрытие. Однако не все данные требуют одинаковой защиты. Например, само по себе имя учащегося не так уязвимо, как его социальное положение или имя в сочетании с медицинской информацией. При этом защита личной информации имеет первостепенное значение. Тем не менее учебная организация в силах помочь сохранить информацию в безопасности или без должного отношения к безопасности открыть к ней доступ тем, кто может причинить вред. Таким образом, ответственность заключается в том, чтобы придерживаться строгих требований безопасности образовательного учреждения, чтобы сохранить данные от посторонних глаз. Высокоуровневые требования к соблюдению принципа безопасности в России определены, прежде всего, ФЗ «О персональных данных» [11]. Далее эти требования «конкретизированы в подзаконных актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России) и Федеральной службы по надзору в сфере связи и массовых коммуникаций (Роскомнадзор)» [13].

Пятый принцип – **качество данных и целостность**. Неточные или устаревшие данные бесполезны и могут навредить. Например, если у вас когда-то был плохой кредитный рейтинг, и вы предпринимали шаги по его улучшению на протяжении многих лет, а ваши кредиторы все еще использовали устаревшую информацию, такой подход может навредить вам и ограничить ваши возможности. То же самое относится и к нашим учащимся. Информация, которой располагает образовательное учреждение о них, должна оставаться актуальной и точной. Таким образом, любое образовательное учреждение, создающее, поддерживающее, использующее или распространяющее записи идентифицируемых персональных данных, должна гарантировать надежность таких данных для их предполагаемого использования и должна принимать меры предосторожности для предотвращения неправильного их использования.

Политики и процессы обработки личной информации необходимы, но, если мы не будем следить за тем, как сотрудники в организации соблюдают эти политики и процессы, мы не будем знать, как идут дела по соблюдению принципов конфиденциальности. Поэтому, чтобы нести ответственность за соблюдение этих принципов, требуется наладить дисциплину контроля. Поэтому **обеспечение контроля** следует выделить в качестве шестого ключевого принципа конфиденциальности.

2.3. Обеспечение конфиденциальности в цифровой образовательной среде

Как может быть обеспечена защита личной информации обучающегося в соответствии с указанными в п. 2.2 ключевыми принципами в цифровой образовательной среде? Чтобы ответить на этот вопрос проанализируем принципы обеспечения контроля, доступа, ограничения использования и прозрачности в действии в цифровой образовательной среде. Использование той или иной образовательной платформы зависит от определенных договоренностей с внешними поставщиками таких услуг, как, например, предоставление

облачного хранилища или встроенной функции аналитики данных, или видеопроигрывателя и т.д. Одновременно, использование образовательной платформы (поставщиком ресурса) учебным заведением также регламентируется между ними определенными договорными требованиями. Для того, чтобы запустить выполнение этих требований, со стороны учащегося достаточно щелкнуть мышью в части принятия условий по передаче личной информации. Здесь важно, чтобы учебное заведение непосредственно контролировало поставщика на предмет использования личной информации учащегося только для целей школы. Осуществить такой контроль можно на основании прописанных прав и обязанностей в соглашении о сотрудничестве.

Требования **к доступу** к личной информации обучающегося, как правило, имеют ограничительный характер. Сводятся они к перечню определенных лиц, которые могут получить данный доступ для выполнения востребованных учебным заведением функций. При этом учебное заведение само должно определить, какую информацию оно считает необходимой для использования в образовательных интересах. Также учебное заведение может квалифицировать физическое или юридическое лицо в качестве школьного должностного лица, которому считает возможным предоставлять личную информацию учащихся. Кроме того, требуется разработать права доступа родителей к личной информации их детей с тем, чтобы иметь возможность просматривать и запрашивать по необходимости исправление ошибок в учебе своего ребенка. Принцип доступа также действует, когда приходится решать такие технологические вопросы, как запрет учащимся со стороны учебного заведения предоставлять свои пароли для личных устройств или аккаунтов в социальных сетях.

Принцип **ограничения** использования связан, прежде всего, с ограничением использования информации в коммерческих целях. В России пока не существуют государственных законов, которые запрещали бы использование личной информации учащихся в целях "таргетированной рекламы". В цифровом пространстве процесс коммерциализация персональных данных происходит достаточно быстро. Тем временем «в ст. 8 Хартии Европейского союза об основных правах закреплено, что каждый имеет право на защиту относящихся к нему персональных данных. Обработка подобных данных должна производиться добросовестно в четко определенных целях с согласия заинтересованного лица либо при наличии других оснований, предусмотренных законом» [14].

И, наконец, общие требования к соблюдению принципа **прозрачности** сводятся к пониманию механизма защиты персональной информации учащегося. Различные законодательные акты о конфиденциальности данных требуют, чтобы компании, в т.ч. и государственные образовательные учреждения, разрабатывали политику управления личными данными, которая призвана способствовать защите конфиденциальности данных учащихся (далее политика конфиденциальности). Ожидается, что такая политика будет доступной для родителей. Кроме того, еще одной ключевой областью прозрачности может быть уведомление соответствующих инстанций о случае несанкционированного доступа к персональной информации учащихся, представляющего собой нарушение **безопасности**.

Таким образом, важность соблюдения принципов конфиденциальности в цифровой образовательной среде налицо. Несмотря на то, что некоторые законы о конфиденциальности уже вступили в силу в России, есть условия, требующие дальнейшего расследования для решения оставшихся без ответа вопросов, включая обеспечение соблюдения рассмотренных принципов конфиденциальности.

3. Рекомендации по обеспечению личной безопасности обучающегося

3.1. Условия использования цифровых образовательных ресурсов

Противоречивая задача возникает у администрации учебных заведений по обеспечению личной безопасности своих учащихся. С одной стороны, есть законы, регламентирующие

защиту персональных данных, с другой – сложно понять, как имеющиеся юридические требования переводить в руководства для повседневного использования, чтобы исключить проблемы, связанные с утечкой личной информации учащихся. Доступность различных цифровых образовательных ресурсов и веб-сайтов усугубляют решение этой задачи. Тем временем, ответственность за соблюдение вышеуказанных принципов не снимается с плеч администрации учебного заведения, решению которой может помочь понимание того, какими технологиями мы пользуемся на занятиях с учащимися. Ключевым обязательством использования такой технологии выступает обязательство надлежащей проверки на предмет обеспечения конфиденциальности и безопасности использования личной информации учащегося. Это первое условие использования цифровых образовательных ресурсов в работе с учащимися.

Развитие преподавания в цифровой образовательной среде предполагает использование различных цифровых инструментов. Выбор того или иного приложения зависит от образовательной цели, которую мы стремимся достичь на занятии. Однако, надо понимать, что само по себе использование цифровых технологий в работе не является чем-то инновационным. Новаторство будет состоять в том, как, используя то или иное приложение, мы достигаем образовательной цели? В чем можно измерить эффективность использования технологического ресурса? Ответы на эти вопросы помогут обосновать искомый выбор и одновременно являются вторым условием в данном случае в контексте выбора ресурса.

Повторим: чтобы получить доступ к приложению, необходимо согласиться с онлайн-условиями и политикой конфиденциальности поставщика технологии, поставив галочку в соответствующем окне. С учетом юридических требований поставщики ресурсов запрашивают согласие с условиями их использования. Часто пользователи не глядя кликают в окошке, подтверждая свое согласие с этими условиями. Это неверно. Важно обязательное чтение документа и подписание его только после осмысления прочитанного. Это третье условие использования цифровых образовательных приложений в работе с учащимися.

Теперь затронем вопрос учетной записи. Когда учащийся создает учетную запись, он вписывает туда свою личную информацию. Это требуется для обеспечения контроля над успеваемостью каждого обучающегося со стороны учебного заведения. Отсюда возникает вопрос, насколько можно доверять поставщику технологии в части обеспечения конфиденциальности персональных данных учащихся и как гарантировать неразглашение этой информации? Если в качестве поставщика технологии выступает орган исполнительной власти, то он сам имеет интерес, например, в статистических и/или аналитических данных учащихся. А если это частная технология?.. Поэтому важным представляется на уровне самого учебного заведения разработка политики конфиденциальности, в которой прописываются права и обязанности разного уровня поставщиков. В частности, поставщик технологий должен использовать персональную информацию об учащихся только для того, чтобы поддержать законные образовательные интересы. Гарантии того, что поставщик технологий будет делать с персональной информацией студентов, должны быть сформулированы в политике конфиденциальности – это четвертое условие использования цифровых образовательных приложений в работе с учащимися. Кроме этого, в политике конфиденциальности требуется прописать информацию о третьих сторонах, работающих с технологическим ресурсом, и о том, как поставщик технологий должен управлять соблюдением конфиденциальности личной информации учащихся.

3.2. Рекомендации при разработке политики конфиденциальности

Итак, чтобы максимально учесть образовательные интересы и обеспечить личную безопасность учащихся в цифровой образовательной среде в учебном заведении требуется разработать политику конфиденциальности. Вот некоторые шаги, которые помогут предусмотреть негативные последствия в части разглашения и/или использования в коммерческих целях личной информации школьников/студентов/пользователей.

Сначала необходимо провести полную ревизию всех цифровых образовательных ресурсов, а также других веб-сайтов, планируемых к использованию на занятиях в рамках той или иной дисциплины, и выбрать на ваш взгляд более подходящие с точки зрения методики использования их на занятии. Далее следует ознакомиться с предлагаемой политикой конфиденциальности поставщиков выбранных ресурсов и отобрать те, которые обеспечивают личную безопасность учащихся. Обобщим критерии исключения цифровых образовательных ресурсов для использования на занятии:

— политика конфиденциальности поставщика ресурса не соответствует существующим законам о конфиденциальности и/или требованиям к обеспечению личной безопасности, предъявляемым самим учебным заведением;
— данный ресурс предназначен для пользователей, которые старше, чем те, для которых планируется его использовать;
— учебное заведение не может контролировать записи учащихся, которыми управляет поставщик ресурса;
— данные, передаваемые поставщику ресурса, не будут защищены надлежащим образом.

Учет указанных критериев позволяет предусмотреть риск разглашения и/или передачи личной информации учащихся третьим лицам или ее использования в коммерческих целях.

Конечно, это не универсальные и исчерпывающие меры для обеспечения личной безопасности учащегося в цифровой образовательной среде. Тем не менее, они позволяют развивать навыки работы с рекомендуемыми цифровыми педагогическими практиками в части обеспечения личной безопасности учащегося на протяжении всего процесса обучения.

4. Заключение

Таким образом, в работе предложены рекомендации при разработке политики конфиденциальности на уровне учебного заведения. Для этого проанализированы некоторые примеры поведения, которые могут поставить под угрозу конфиденциальность или безопасность персональных данных в новой цифровой образовательной среде, дана качественная оценка прямым и косвенным факторам идентификации, проанализированы основные принципы надлежащей информационной практики FIPP в контексте их соблюдения в существующих законодательных актах РФ. В результате работы было определено сходство работы принципов, обеспечивающих личную безопасность в традиционной и цифровой образовательной среде, рассмотрены с различных точек зрения условия использования цифровых образовательных ресурсов, а также предложены критерии их исключения из планируемого перечня используемых на занятиях.

Указанные меры могут быть использованы при формировании политики конфиденциальности в учебном заведении для обеспечения личной безопасности в цифровой образовательной среде при реализации соответствующих педагогических практик. Пользоваться данными рекомендациями могут педагоги не только школ, но и преподаватели высших учебных заведений, что будет способствовать повышению осведомленности и заинтересованности с их стороны осознанно управлять личной безопасностью обучающихся, сохраняя конфиденциальность данных.

Литература

[1] Эксперты оценили объем «утечек» персональных данных россиян в 2020 году. // Ведомости: технологии. 2021. 11 января. URL: https://www.vedomosti.ru/technology/news/2021/01/11/853607-eksperti-otsenili-obem-utechek-personalnih-dannih-rossiyan-v-2020-godu (дата обращения: 14.06.2021).
[2] «Защити меня» // PwC в России: исследования. 2018. URL: https://www.pwc.ru/protectme2018 (дата обращения: 14.06.2021).

[3] Персональные данные потребителей: когда частное становится публичным // KPMG: исследование по вопросам неприкосновенности частной жизни. 2017. URL: https://assets.kpmg/content/dam/kpmg/ru/pdf/2017/01/ru-ru-crossing-the-line-survey.pdf (дата обращения: 14.06.2021).
[4] Солдатова Г.У., Олькина О.И. Отношение к приватности и защита персональных данных: вопросы безопасности российских детей и подростков // Национальный психологический журнал. 2015. № 3 (19). С. 56-66.
[5] Larry Ponemon Institute Research Report, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT". Ponemon Institute Cost of a Data Breach Study 2018, July 11, 2018. URL: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ (дата обращения: 14.06.2021).
[6] Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 29.12.2020). Доступ из справ.-правовой системы «КонсультантПлюс».
[7] Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
[8] Перечень конфиденциальной информации // HR-Portal: корпоративная культура. 2012. 18 окт. URL: https://hr-portal.ru/article/perechen-konfidencialnoy-informacii (дата обращения: 14.06.2021).
[9] Готовое решение: что относится к конфиденциальной информации [Электронный ресурс]: (КонсультантПлюс, 2021). Доступ из справ.-правовой системы «КонсультантПлюс».
[10] Privacy Policy Guidance Memorandum: The Fair Information Practice Principles. URL: https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf (дата обращения: 14.06.2021).
[11] Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
[12] Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».
[13] Искусство управления информационной безопасностью // ISO27000.ru. 2021. URL: http://iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/zaschita-personalnyh-dannyh (дата обращения: 14.06.2021).
[14] Урошлева А. Коммерциализация персональных данных и понятие "биг дата" – злободневные вопросы IT-сферы // Гарант.ру. 22 ноября 2018 г. URL: http://www.garant.ru/article/1229761/#ixzz6pIjSbMku (дата обращения: 14.06.2021).

Personal safety of students in the digital educational environment

A.N. Rasskazova[1], A.S. Zykova[2]

[1] North-Western State Medical University named after I.I. Mechnikov,
[2] Sevastopol State University

We, as teachers, have the right and access to daily collection and processing of student data. At the same time, along with the development of new digital technologies for data collection and processing, it is important to respect their confidentiality and the duty to protect. Although protecting the confidentiality of students' data is part of the primary responsibility to care for them, not all educational institutions have written agreements and/or guidelines on data protection, as well as any provisions regarding the collection and use of private information.
Thus, the purpose of this work is to propose recommendations for the development of a privacy policy directly in educational institutions. To do this, the role of the teacher in protecting student data from the point of view of informed information management is analyzed and a number of measures are discussed to protect the confidentiality of student data, without violating the

educational goals and style of the teacher. The subject of analysis are students of the general education system, students of secondary special and higher educational institutions.

Keywords: personal data, access, control, transparency, restriction of use, digital educational resources

Reference for citation: Rasskazova A.N., Zykova A.S. Personal safety of students in the digital educational environment // Information Society: Education, Science, Culture and Technology of Future. Vol. 5 (Proceedings of the XXIV International Joint Scientific Conference «Internet and Modern Society», IMS-2021, St. Petersburg, June 24-26, 2021). - St. Petersburg: ITMO University, 2021. P. 85 – 94. DOI: 10.17586/2587-8557-2021-5-85-94

Reference

[1] Experts estimated the volume of "leaks" of personal data of Russians in 2020 // Vedomosti: technologies. 2021. January 11. URL: https://www.vedomosti.ru/technology/news/2021/01/11/853607-eksperti-otsenili-obem-utechek-personalnih-dannih-rossiyan-v-2020-godu (access date: 14.06.2021).

[2] Protect Me // PwC in Russia: research. 2018. URL: https://www.pwc.ru/protectme2018 (access date: 14.06.2021).

[3] Consumer Personal Data: When Private Becomes Public //KPMG: Privacy Research. 2017. URL: https://assets.kpmg/content/dam/kpmg/ru/pdf/2017/01/ru-ru-crossing-the-line-survey.pdf (access date: 14.06.2021).

[4] Soldatova G.U., Olkina O.I. Attitude to privacy and protection of personal data: security issues of Russian children and adolescents // National Psychological Journal. 2015. № 3 (19). P. 56-66.

[5] Larry Ponemon Institute Research Report, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT": Ponemon Institute Cost of a Data Breach Study 2018, July 11, 2018. URL: https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/ (access date: 12.06.2021).

[6] Labor Code of the Russian Federation of 30.12.2001 N 197-FZ (as amended. from 29.12.2020). Access from the help.- the legal system "ConsultantPlus".

[7] Federal Law "On Commercial Secrets" of 29.07.2004 N 98-FZ. Access from the help.- the legal system "ConsultantPlus".

[8] List of confidential information // HR-Portal: corporate culture. 2012. 18 Oct. URL: https://hr-portal.ru/article/perechen-konfidencialnoy-informacii (access date: 10.03.2021).

[9] Ready-made solution: what applies to confidential information: (ConsultantPlus, 2021). Access from the help.- the legal system "ConsultantPlus".

[10] Privacy Policy Guidance Memorandum: The Fair Information Practice Principles [website]. URL: https://www.dhs.gov/sites/default/files/publications/privacy-policy-guidance-memorandum-2008-01.pdf (access date:10.03.2021).

[11] Federal Law "On Personal Data" of 27.07.2006 N 152-FZ. Access from the help.- the legal system "ConsultantPlus".

[12] Code of the Russian Federation on Administrative Offences of 30.12.2001 N 195-FZ. Access from the help.- the legal system "ConsultantPlus".

[13] The art of information security management // ISO27000.ru. 2021. URL: http://iso27000.ru/chitalnyi-zai/zaschita-personalnyh-dannyh/zaschita-personalnyh-dannyh (access date: 10.03.2021).

[14] Uroshleva A. Commercialization of personal data and the concept of "big data" – topical issues of the IT sphere // Garant.ru. November 22, 2018. URL: http://www.garant.ru/article/1229761/#ixzz6pIjSbMku (access date: 10.03.2021).