Электронный журнал

СПРАВОЧНИК
ЗАМЕСТИТЕЛЯ
ДИРЕКТОРА ШКОЛЫ

Работаем с кадрами

Обеспечение информационной безопасности в образовательных организациях

В.В. Толмачев
канд. воен. наук, доц. каф. комплексной безопасности ГБОУ ВПО МО "Академия социального управления", доц., заслуженный военный специалист РФ, г. Москва

Чем обусловлена необходимость обеспечения безопасности информации в ОО? Автор статьи приводит и анализирует все основания. Описывая типы локальных сетей, дает качественные характеристики каждой. Выбор – за ОО.

В статье рассмотрены вопросы, которые чаще всего вызывают затруднения у администрации. Например, на кого возложить обязанности администратора безопасности, если такая должность штатным расписанием ОО вообще не предусмотрена? Все о деятельности ОО по обеспечению безопасности персональных данных и ограничению доступа обучающихся к информации, причиняющей вред их здоровью и развитию.

Нормативно-правовые основы информационной безопасности

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» (далее — Федеральный закон № 273-ФЗ) устанавливает, что права и обязанности руководителя образовательной организации (далее — ОО), его компетенция в области управления ОО определяются в соответствии с законодательством об образовании и уставом ОО (п. 6 ст. 51 Федерального закона № 273-ФЗ).

Важное место в образовательной деятельности руководителя ОО занимает реализация образовательных программ, в т. ч. с применением электронного обучения и дистанционных образовательных технологий (ст. 16 Федерального закона № 273-ФЗ). При организации образовательной деятельности широко используются компьютеры, информационно-телекоммуникационные сети, аппаратно-программные и аудиовизуальные средства, печатные и электронные образовательные и информационные ресурсы и иные материальные объекты.

На эффективность использования в образовательной деятельности электронных образовательных и информационных ресурсов влияют многие факторы:

- их качество и структурированность;
- разграничение доступа к электронным ресурсам обучающихся и педагогических работников;
- своевременная актуализация информации; защищенность баз данных от уничтожения и искажения и др.

Руководитель ОО оказывается перед необходимостью решения специфической практической задачи — обеспечения информационной безопасности.

В соответствии с **Доктриной информационной безопасности Российской Федерации**, утв. Президентом РФ 09.09.2000 № Пр-1895, одной из составляющих национальных интересов РФ в информационной сфере является развитие современных информационных технологий, отечественной индустрии информации, в т. ч. индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Согласно Положению о Федеральной службе по техническому и экспортному контролю, утв. Указом Президента РФ от 16.08.2004 № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю», Федеральная служба по техническому и экспортному контролю (далее — ФСТЭК РФ) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности. ФСТЭК РФ обеспечивает безопасность (некриптографическими методами) информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере, в т. ч. в функционирующих в составе критически важных объектов РФ информационных системах и телекоммуникационных сетях, деструктивные информационные воздействия на которые могут привести к значительным негативным последствиям.

Руководящие документы ФСТЭК РФ определяют безопасность информации как состояние информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования и блокирования[1].

Статья 29 Федерального закона № 273-ФЗ, определяя информационную открытость ОО, устанавливает ограничения на информацию и документы, составляющие государственную и иную охраняемую законом тайну. Федеральный закон № 273-ФЗ предусматривает полную информационную открытость и доступность только в отношении информации о системе образования РФ, что закреплено в ст. 97.

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обеспечение безопасности информации в ОО

Необходимость **обеспечения безопасности информации в ОО** обусловлена несколькими обстоятельствами. Во-первых, ст. 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее — Федеральный закон № 149-ФЗ) определяет, что информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен, и называет ее *информацией ограниченного доступа*, распространение которой в РФ ограничивается или запрещается (ст. 5). Такая информация, к примеру, содержится в контрольных измерительных материалах, используемых при проведении государственной итоговой аттестации, что закреплено ч. 11 ст. 59 Федерального закона № 273-ФЗ.

Указом Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» введено понятие *служебной тайны*: «служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами» (п. 3). Также понятие «служебная тайна» определено Федеральным законом № 149-ФЗ: «федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение» (п. 4 ст. 9).

Пункт 7 ст. 2 Федерального закона № 149-ФЗ устанавливает понятие *конфиденциальности информации* — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Такого рода информация в ОО содержится в персональных данных

педагогических работников и обучающихся, в документах по усыновлению, налоговых, банковских, медицинских и других документах; в документах по антитеррористической защищенности, гражданской обороне, по действиям в чрезвычайных ситуациях.

Во-вторых, образование, как единый целенаправленный процесс воспитания и обучения, неразрывно связано с информацией, используемой в научных, учебных или культурных целях, а также с электронным обучением и дистанционными образовательными технологиями. Неправомерные действия в отношении такой общедоступной информации могут привести к нарушению или даже к временной приостановке образовательной деятельности ОО.

В-третьих, в ОО возникает необходимость не только защиты информации, но и защиты обучающихся от информации, причиняющей вред их здоровью и развитию. Статья 2 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (далее — Федеральный закон № 436-ФЗ) определяет, что «информация, причиняющая вред здоровью и (или) развитию детей, — информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом». Виды информации, причиняющей вред здоровью и развитию детей, перечислены в ст. 5 Федерального закона № 436-ФЗ. В части 4 ст. 2 Федерального закона № 436-ФЗ представлено определение *информационной безопасности детей* как состояния защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Таким образом, в ОО, наряду с необходимостью защиты информации, актуальной является задача ограничения доступа обучающихся к информации, причиняющей вред их здоровью и развитию. Последнее относится к информации, поступающей из сети Интернет.

Часть 4 ст. 6 Федерального закона № 149-ФЗ возлагает обязанности по защите информации и ограничению доступа к ней на обладателя информации, т. е. на ОО. Аналогичные требования содержатся и в ч. 5 ст. 16 Федерального закона № 273-ФЗ: «При реализации образовательных программ с применением электронного обучения, дистанционных образовательных технологий организация, осуществляющая образовательную деятельность, обеспечивает защиту сведений, составляющих государственную или иную охраняемую законом тайну».

Исследование состояния защиты информации

Сотрудниками кафедры комплексной безопасности ГБОУ ВПО МО «Академия социального управления» проведено исследование состояния защиты информации в информационных системах ОО Центрального федерального округа в части использования вычислительной техники, информационных систем, а также состояния

защиты информации и персональных данных. Результаты исследования показали, что количество персональных компьютеров (далее — ПК) в ОО колеблется в пределах от 20 до 170 ед. Однако их структурирование в локальные вычислительные сети существенно разнится: от 22 до 100%. В среднем по регионам в локальные вычислительные сети объединены 65% компьютеров ОО, а 35% используются в качестве персональных рабочих станций.

Необходимо отметить, что объединение персональных компьютеров в локальные вычислительные сети не только является необходимым условием повышения эффективности их использования, но и обеспечивает централизацию политики защиты служебной информации. Немаловажное значение для организации защиты информации имеет и тип локальной сети. В подавляющем большинстве ОО (72%) персональные компьютеры объединены в простейшие одноранговые локальные сети, в 21% ОО — локальные вычислительные сети построены по клиент-серверной архитектуре и лишь 7% сетей имеют доменную структуру.

Типы локальных сетей и их использование

Одноранговая (одноуровневая) локальная сеть — это сеть равноправных компьютеров (рабочих станций), каждый из которых имеет уникальное имя и пароль для входа. В одноранговой сети каждая рабочая станция может разделить все ее ресурсы с другими рабочими станциями сети. Рабочая станция может разделить часть ресурсов, а может и вообще не предоставлять никаких ресурсов другим станциям. Каждый пользователь одноранговой сети является администратором на своем компьютере. Настроить групповую политику безопасности в такой сети чрезвычайно сложно.

Клиент-серверная архитектура локальной сети представляет собой более совершенную распределенную двухуровневую вычислительную сеть. Клиент-серверная архитектура состоит в простейшем случае из трех основных компонентов:

- сервер баз данных, управляющий хранением данных, доступом и защитой, резервным копированием, отслеживающий целостность данных в соответствии с бизнес-правилами и выполняющий запросы клиента;
- клиент, предоставляющий интерфейс пользователя, посылающий запросы к серверу и получающий ответы от него;
- сеть и коммуникационное программное обеспечение, осуществляющее взаимодействие между клиентом и сервером посредством сетевых протоколов.

Такую архитектуру сети, к примеру, использует универсальная бухгалтерская программа 1С, а также файловые серверы, серверы печати, почтовые серверы, веб-серверы и др.

Наиболее совершенной с точки зрения реализации локальных и групповых политик безопасности представляется **сеть с контроллером домена**. Контроллер домена

в компьютерных сетях — это сервер, контролирующий область компьютерной сети (домен). Контроллер домена хранит параметры учетных записей и паролей пользователей, параметры безопасности файлового хранилища, параметры групповой и локальной политик безопасности для разграничения прав доступа пользователей в сети к информационным ресурсам.

Сервер контроллера домена позволяет не только свести к минимуму риски несанкционированного доступа и хищения информации, но и надежно защитить ее от утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования и блокирования. Это в значительной мере достигается разграничением доступа к файловому массиву ОО и настройкой автоматической архивации данных, а также подключением сервера к сети через источник бесперебойного питания. У локальной сети с контроллером домена только один недостаток: необходима дополнительная подготовка специалистов для настройки и администрирования доменных сетей. К сожалению, подготовке таких специалистов для ОО пока уделяется недостаточное внимание.

Проблемы администрирования локальных вычислительных сетей

В общепринятой практике администрирование локальных вычислительных сетей возлагается на администратора, а для надежной защиты конфиденциальной информации и персональных данных **вводятся должности администраторов безопасности**. Такие должности штатными расписаниями ОО не предусмотрены. Не содержатся такие требования и в «Типовой должностной инструкции заместителя руководителя организации, осуществляющей образовательную деятельность, по безопасности образовательного процесса»[2] (далее — Инструкция). Содержащееся в п. 3.2 Инструкции требование «обеспечивать сохранность служебной информации и персональных данных обучающихся и работников организации» относится к документам на бумажных носителях, а не к данным, обрабатываемым в информационных системах ОО, т. к. в ст. 1.5 Инструкции не содержатся нормативные правовые документы по защите информации и защите детей от информации, причиняющей вред их здоровью и развитию.

Руководители ОО пытаются найти выход из сложившейся ситуации, давая учителям информатики и информационно-коммуникационных технологий (далее — ИКТ) разовые поручения, например, по отправке адресату бухгалтерских документов с использованием электронной цифровой подписи. Но при этом необходимо признать, что информатика и ИКТ и администрирование сетей соотносятся так же, как литература и математика. Не представляется возможным осуществлять обслуживание локальных сетей путем фрагментарных обращений к «продвинутым пользователям» из числа других работников ОО, т. к. приходится раскрывать систему парольной защиты. Не могут решить проблему информационной безопасности и другие вынужденные «административные уловки»

руководителей ОО, когда для обслуживания компьютерных сетей ОО привлекаются родители (законные представители) обучающихся или обучающиеся старших классов.

Отдельного рассмотрения требует **проблема аутентификации**. Аутентификация пользователя — это проверка, действительно ли пользователь является тем, за кого он себя выдает. В ОО, как правило, используется однофакторная аутентификация — задание пользователем паролей.

Пароль — это просто набор символов. Чаще всего у системы нет другого способа узнать вас, кроме как по паролю. Следовательно, кто угодно может ввести правильный пароль и получить соответствующие полномочия. Пароль может быть *узнан, угадан* или *подобран*. Не будем рассматривать ситуации, когда «пароль» задается в виде последовательности числового ряда из 3–9 цифр. Многие пользователи при выборе пароля исходят из удобства его *произносимости и запоминаемости*. Такие пароли не являются преградой не только для хакеров, но и для продвинутых пользователей.

Две главных характеристики пароля — количество символов (длина) и количество вариантов символа в каждой позиции (алфавит). Так, при использовании латиницы разного регистра с учетом цифр мы можем применить для задания пароля 62 символа. Расчеты показывают, что при данном условии стойкость пароля может составить:

- при длине пароля в 10 символов — 2 г. и 8 мес.;
- 8 символов — 252 сут.;
- 6 символов — 95 мин.

С учетом изложенного выше, при задании пароля доступа к компьютеру или серверу, особенно содержащему базу данных или конфиденциальную информацию, необходимо руководствоваться следующими правилами:

- пароль должен содержать не менее 8 символов латиницы и двух цифр;
- латиница должна содержать хотя бы одну букву другого регистра;
- набор букв латиницы не должен составлять слово из любого известного словаря.

Чтобы пароль был надежным и легко запоминаемым, целесообразно использовать при его наборе и другие разрешенные символы (. , — ! ? и т. п.). Так, например, стойкость пароля *Kb-54-kB* при указанных выше условиях составит не менее 2 лет.

Необходимо также, чтобы все компьютеры ОО имели как минимум две учетные записи: администратора и пользователя, причем с отдельным паролем каждая.

В ходе наших исследований было установлено, что у руководителей ОО отсутствуют распечатки паролей администраторов компьютерного и сетевого оборудования, ввиду отсутствия работника, которому это вменено в должностные обязанности. Ежедневные

резервные копирования информационных ресурсов и системы восстановления работоспособности программного обеспечения реализованы лишь в отдельных ОО. Для выполнения этой работы необходим администратор сети, в полной мере отвечающий требованиям *лояльности и надежности*.

Важную роль в защите информации на компьютерах занимают антивирусные программы. В ходе исследования нами установлено, что на всех ПК в ОО используется антивирусное программное обеспечение Dr. Web или антивирус Касперского. Однако в некоторых ОО используется предустановленное производителем компьютеров антивирусное программное обеспечение McAfee (США). Этот антивирус может автоматически оформить подписку на обновление и будет снимать деньги со счета без уведомления пользователя.

Защита персональных данных

Отдельной проблемой для ОО является **необходимость защиты персональных данных**. Статья 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» определяет обеспечение безопасности персональных данных как комплексную задачу, которая включает:

- определение угроз безопасности персональных данных;
- применение как организационных, так и технических мер защиты;
- применение сертифицированных средств защиты информации;
- учет машинных носителей персональных данных;
- предотвращение несанкционированного доступа к персональным данным и обеспечение регистрации и учета всех действий, совершаемых с персональными данными, и другие меры.

В ходе экспертного опроса 43% респондентов ОО утвердительно ответили на вопрос: «Уведомила ли вас ОО о начале обработки персональных данных в защищенном режиме?». Однако сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее — Роскомнадзор России) не подтверждает этих данных. Поиск организаций на сайте Роскомнадзора России формирует по регионам список только 6,4% ОО от их общего числа.

Это свидетельствует о том, что большинство ОО ограничиваются локальными, фрагментарными мерами по защите персональных данных, которые зачастую сводятся к получению письменного согласия субъекта на обработку персональных данных и разработке политики оператора в вопросах обработки персональных данных, что нельзя признать достаточным уровнем их защиты.

Надлежащая защита персональных данных обходится достаточно дорого. Стоимость оборудования и работ, по опыту выполняющих их организаций, составляет от 400 тыс. до 1,5 млн руб. Такими финансовыми ресурсами ОО в настоящее время не располагают.

На наш взгляд, не обеспечит требуемый уровень защиты персональных данных и использование аутсорсинга. Разумеется, специализированная организация справится с защитой персональных данных должным образом. Но их источником и конечным пользователем остается ОО. Это обусловливает необходимость создания защищенных каналов связи, защиты информации в локальной сети и на рабочих станциях должностных лиц ОО, что практически приведет к удвоению стоимости системы защиты информации.

В качестве одного из начальных условий защиты персональных данных в ОО можно рекомендовать использование на соответствующем рабочем месте оператора персональных данных двух системных блоков, один из которых подключен к локальной вычислительной сети и, соответственно, к сети Интернет, а другой — используется как отдельная защищенная персональная рабочая станция. При этом клавиатура, монитор и мышь могут коммутироваться посредством KVM-переключателя, сертифицированного по требованиям информационной безопасности.

Кроме того, один из сотрудников ОО должен пройти обучение в специализированной организации и получить свидетельство администратора безопасности.

Ограничение доступа обучающихся к информации, причиняющей вред здоровью и развитию

Несколько слов об **ограничении доступа обучающихся к информации, причиняющей вред их здоровью и развитию**. В ходе исследования установлено, что все ОО имеют широкополосный доступ к сети Интернет (от 1 до 100 Мбит/сек). Для ограничения доступа к нежелательному контенту примерно 60% ОО используют услуги провайдеров. В остальных ОО применяются специальные фильтры NetPolice (разработка российской компании «Центр анализа интернет-ресурсов») либо используют возможности программируемых маршрутизаторов. Все эти меры, там, где они реализованы, позволяют решить поставленную задачу с достаточной надежностью. Руководителям ОО следует избегать использования технологии Wi-Fi для беспроводного доступа обучающихся и персонала к сети Интернет.

Таким образом, в вопросах практической реализации требований информационной безопасности в ОО проделана определенная работа. Тем не менее ее результаты пока еще не в полной мере соответствуют требованиям федеральных законов и других нормативных правовых актов в части обеспечения информационной безопасности.

Учитывая то, что решение многих из рассмотренных проблем обеспечения информационной безопасности зависит от компетенции администрации ОО, членам администрации ОО целесообразно повысить квалификацию на соответствующих курсах повышения квалификации по программе «Информационная безопасность

в общеобразовательной организации». Программа должна быть ориентирована на администрацию ОО и особенно на заместителей руководителя ОО по безопасности. При этом в программе должны быть учтены основные положения приказов Минобрнауки России:

- от 28.10.2009 № 497 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) „магистр“)»;
- от 17.01.2011 № 60 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки (специальности) 090303 Информационная безопасность автоматизированных систем (квалификация (степень) „специалист“)».

Целью программы необходимо определить качественное повышение профессиональной компетенции руководящих работников ОО в вопросах обеспечения информационной безопасности электронных образовательных ресурсов, а также защиты детей и подростков от информации, причиняющей вред их здоровью и развитию. Актуальность и особенность программы должна быть в ее доступности для усвоения членами администрации ОО, которые не являются специалистами в сфере ИКТ и защиты информации, а имеют лишь навыки пользователя.

На примере компьютерных сетей ОО в ходе занятий необходимо рассмотреть современные средства и способы защиты информации и персональных данных. Особое внимание целесообразно уделить работе руководителя ОО по планированию, организации и практической реализации требований информационной безопасности, включая разработку необходимых нормативных документов.

Руководитель ОО должен знать и правила размещения на официальном сайте информации об ОО, которые определены постановлением Правительства РФ от 10.07.2013 № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети Интернет и обновления информации об образовательной организации». Для комплексного решения проблемы информационной безопасности ОО необходимо также изыскать дополнительные возможности для кадрового обеспечения администрирования локальных вычислительных сетей и информационных ресурсов ОО.

[1]Приказ ФСБ РФ № 416, ФСТЭК РФ № 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования». *>>вернуться в текст*

[2]Письмо Минобрнауки России от 14.02.2014 № МК-169/12 «О типовой должностной инструкции заместителя руководителя организации, осуществляющей образовательную деятельность, по безопасности». *>>вернуться в текст*