Информационная безопасность школы

В последние годы в школах участились попытки несанкционированного получения информации, в т. ч. персональных данных педагогов и учащихся. Противодействовать такой тенденции можно, создав в образовательном учреждении систему информационной безопасности.

Нынешнее столетие характеризуется особенностью перехода от индустриального общества к информационному. В этих условиях тот, кто обладает информацией и умело ее использует, способен оперативно решать поставленные задачи, организовывать работу подчиненных, обеспечивать успешное развитие своего предприятия.

Информация и обеспечивающие ее системы и сети являются ценными ресурсами. Собственники информации сталкиваются с возрастающей угрозой нарушения режима безопасности, исходящей из различных источников. Информационным системам и сетям могут угрожать такие опасности, как: компьютерное мошенничество, компьютерные вирусы, хакеры, вандализм, хищение, разглашение конфиденциальной информации и другие виды угроз. В процентном отношении, по различным оценкам специалистов, данные угрозы в среднем распределяются следующим образом:

- разглашение информации в результате подкупа работников – 43%;
- копирование программ и данных – 24%;
- проникновение в ПЭВМ – 18%;
- подслушивание переговоров – 5%.

Анализ состояния дел в области информационной безопасности позволяет сделать вывод, что система мер, обеспечивающая защиту информации, значительно уменьшает возможность ее утечки, несанкционированного доступа, разглашения и потери информации. Главным является обеспечение бесперебойной работы организации и сведение к минимуму ущерба от событий, таящих угрозу информационной безопасности.

Тем не менее опыт показывает, что число попыток, направленных на несанкционированное получение информации, не сокращается, а имеет устойчивую тенденцию к росту. Для успешного противодействия этой тенденции необходима стройная и управляемая система информационной безопасности (далее – СИБ).

СИБ должна обязательно обеспечивать:

- **конфиденциальность** (защиту информации от несанкционированного раскрытия или перехвата);
- **целостность** (точность и полноту информации и компьютерных программ);
- **доступность** (возможность получения пользователями информации в пределах их компетенции).

С учетом зарубежного и отечественного опыта обеспечение информационной безопасности осуществляется по следующим направлениям:

- правовая защита – это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита – это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба;
- инженерно-техническая защита – это использование различных технических средств, препятствующих нанесению ущерба.

При построении системы информационной безопасности решающую роль играет организационная защита. В первую очередь необходимо учесть следующие аспекты:

1. Безопасность информации может быть обеспечена при комплексном использовании всего арсенала имеющихся средств защиты.
2. Никакая система защиты информации не может обеспечить требуемого уровня безопасности информации без соответствующей подготовки пользователей и соблюдения ими установленных правил.
3. Процесс построения системы информационной безопасности не является разовым мероприятием. Он должен постоянно совершенствоваться, быть управляемым. Такой подход является главным стратегическим звеном во всей системе информационной безопасности, а информация – главным элементом защиты.

Следует помнить, что информация существует в различных формах. Ее можно хранить на компьютерах, передавать по локальным сетям и через Интернет, распечатывать на бумажных носителях, копировать, сканировать, а также озвучивать в разговорах. В целях безопасности все виды носителей информации (документы, пленки, магнитные ленты, дискеты, диски и др.), используемые для ее хранения, должны быть надлежащим образом защищены.

Очень часто, рассматривая информационную безопасность, путают и отождествляют два понятия: "компьютерная безопасность" и "информационная безопасность". Это неверно. "Компьютерная безопасность" очень важна, но она является только одной из составляющих "информационной безопасности".

Какую же работу необходимо проделать образовательному учреждению (далее – ОУ) для обеспечения компьютерной безопасности?

Во-первых, целесообразно обеспечить **защиту** компьютеров **от внешних несанкционированных воздействий** (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.). Решение данной проблемы возможно только при условии, исключающем вывод локальных сетей ОУ на Интернет, либо размещение своего сайта у удаленного провайдера.

Во-вторых, необходимо **иметь как минимум два сервера**. Наличие хороших серверов позволит протоколировать любые действия работников ОУ в вашей локальной сети.

В-третьих, необходимо установить **строгий контроль за электронной почтой**, обеспечив постоянный контроль за входящей и исходящей корреспонденцией.

Нелишним будет **установка соответствующих паролей на персональные ЭВМ**, а также определение работы с информацией на съемных носителях ЭВМ (дискеты, диски). И самое главное, класс информатики не должен быть подключен к локальным сетям ОУ.

В дальнейшем могут быть применены и аппаратные средства защиты информации, в т. ч. и ПЭВМ.

В свою очередь, ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях по защите информации" определяет порядок защиты информации. В соответствии с данной статьей защита информации представляет собой принятие правовых, организационных и технических мер. Меры должны быть направлены на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации.

Кроме того, определяется и ответственность граждан за защиту информации. Так, п. 5 ст. 9 Закона № 149-ФЗ гласит: "Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению такой информации".

Такая обязанность возлагается Трудовым кодексом РФ (далее – ТК РФ), гл. 14 которого определяет защиту персональных данных работника. В соответствии со ст. 90 ТК РФ: "Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами".

Для развития данных положений в РФ 27.07.2006 принят Федеральный закон № 152-ФЗ "О персональных данных", который вступил в силу с 1 января 2008 г. Его основной целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в т. ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайны.

Статья 3 данного закона определяет: "Персональные данные – любая информация, относящаяся к определенному или неопределенному на основании такой информации лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация".

Оценивая законодательную базу, следует обратить внимание, что к объектам информационной безопасности в Минобрнауки России, региональных министерствах (департаментах) образования, муниципальных органах управления образованием и в ОУ относят:

- сведения, составляющие государственную тайну, в соответствии с выписками из перечня сведений, подлежащих засекречиванию в министерствах, ведомствах и организациях;
- информационные ресурсы, содержащие документированную информацию, в соответствии с перечнем сведений конфиденциального характера;
- информацию, защита которой предусмотрена законодательными актами РФ, в т. ч. и персональные данные;
- средства и системы информатизации, программные средства, автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом.

Таким образом, можно сделать вывод, что информационная безопасность является одним из составных элементов комплексной безопасности ОУ. Уже сегодня назрела необходимость рассматривать ее как одну из основных составляющих безопасности ОУ.

Учитывая изложенное, под информационной безопасностью ОУ следует понимать состояние защищенности информационных ресурсов, технологий их формирования и использования, а также прав субъектов информационной деятельности.

Построение системы информационной безопасности ОУ происходит следующим образом. На первом этапе определяется, **что подлежит защите**. На втором этапе выявляются возможные **каналы утечки информации** и определяются возможные **угрозы информационным системам**. Далее вырабатываются меры по защите информации и технологических систем. На основе выработанных мер защиты разрабатываются нормативно-правовые документы, регламентирующие информационную безопасность. В последующем организуется контроль за соблюдением установленных правил. При таком подходе система информационной безопасности будет направлена на предупреждение угроз, их своевременное выявление, обнаружение, локализацию и ликвидацию.

В целях обеспечения информационной безопасности и ее организации, на основании законодательных документов, в ОУ следует разрабатывать соответствующие нормативно-правовые акты.

Правовые нормы обеспечения информационной безопасности в конкретном ОУ фиксируются в учредительных, организационных и функциональных документах.

Требования обеспечения информационной безопасности отражаются в уставе (учредительном договоре) в виде следующих положений:

- ОУ имеет право определять состав, объем и порядок защиты сведений конфиденциального характера, персональных данных учащихся, работников ОУ, требовать от своих сотрудников обеспечения сохранности и защиты этих сведений от внешних и внутренних угроз;
- ОУ обязано обеспечить сохранность конфиденциальной информации.

Такие требования дают право администрации ОУ:

- назначить ответственного за обеспечение информационной безопасности;
- издавать нормативные и распорядительные документы, определяющие порядок выделения сведений конфиденциального характера и механизмы их защиты;
- включать требования по обеспечению информационной безопасности в коллективный договор;
- включать требования по защите информации в договоры по всем видам деятельности;
- разрабатывать перечень сведений конфиденциального характера;
- требовать защиты интересов ОУ со стороны государственных и судебных инстанций.

К организационным и функциональным документам следует отнести:

- приказ руководителя ОУ о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников ОУ.

Данный перечень документов не является исчерпывающим. В зависимости от особенностей, специфики и характера ОУ он может быть расширен и дополнен.

Кроме того, должен быть определен порядок допуска сотрудников ОУ к информации. Такой допуск предусматривает:

- принятие работником обязательств о неразглашении доверенных ему сведений конфиденциального характера;
- ознакомление работника с нормами законодательства РФ и ОУ об информационной безопасности и ответственности за разглашение информации конфиденциального характера;
- инструктаж работника специалистом по информационной безопасности;
- контроль работника ответственным за информационную безопасность при работе с информацией конфиденциального характера.

Как показала практика, при проверке организации системы информационной безопасности, как правило, отмечаются следующие недостатки:

- отсутствует перечень сведений, составляющий конфиденциальную информацию;
- отсутствуют должностные обязанности ответственного за информационную безопасность;
- не соблюдается порядок учета носителей информации конфиденциального характера;
- нарушен порядок делопроизводства.

Самым серьезным недостатком в организации информационной безопасности является отсутствие взаимопонимания между теми, кто обеспечивает информационную безопасность, и теми, кто пользуется данной информацией. Нередко пользователи информации нарушают порядок обращения с ней и не соблюдают требования нормативно-правовых документов, регламентирующих информационную безопасность. Решение данной проблемы возможно только при соблюдении принципов информационной безопасности, постоянной требовательности по соблюдению конфиденциальности со стороны руководителя ОУ.

С учетом этих недостатков для обеспечения **информационной безопасности в ОУ требуется проведение следующих первоочередных мероприятий**:

- защита интеллектуальной собственности ОУ;
- защита компьютеров, локальных сетей и сети подключения к системе Интернета в классе информатики ОУ;
- организация защиты конфиденциальной информации, в т. ч. персональных данных работников и учащихся ОУ;
- учет всех носителей конфиденциальной информации.

Реализация данного комплекса мер вносит кардинальные изменения в организацию работы с информационными ресурсами и технологиями, а также делопроизводства, в т. ч. и по вопросам безопасности.

При таком подходе, основными составными задачами делопроизводства станут: документирование информации, учет документов, организация документооборота, обеспечение надежного хранения документов, своевременное их уничтожение, проверка наличия хранящихся документов, контроль за своевременным и правильным их исполнением.

Необходимо помнить, что не на всяком документе имеется гриф "Для служебного пользования" ("Ограниченного пользования"), однако это не означает, что такой документ не представляет никакой ценности. Не бывает важных или не очень важных документов. Самый малозначительный, на первый взгляд документ, при определенных обстоятельствах может оказаться чрезвычайно важным. Организация вышеперечисленных мероприятий позволит избежать непредвиденных ситуаций, путаницы и неразберихи.

Следует отметить, что при организации делопроизводства необходимо выявить и учесть все возможные каналы утечки информации. Наиболее характерными каналами утечки информации для ОУ могут стать разглашение, хищение и несанкционированный доступ.

Учитывая эти аспекты, систему организации делопроизводства можно представить в следующем виде:

- учет всей документации ОУ, в т. ч. и на электронных носителях, с классификацией по сфере применения, дате, содержанию;
- регистрация и учет всех входящих (исходящих) документов ОУ в специальном журнале информации о дате получения (отправления) документа, откуда поступил или куда отправлен, классификация (письмо, приказ, распоряжение и т. д.);
- регистрация документов, с которых делаются копии, в специальном журнале (дата копирования, количество копий, для кого или с какой целью производится копирование);
- особый режим уничтожения документов.

Уничтожать документы можно с помощью уничтожителя бумаг, или сжиганием. В обязательном порядке нужно составлять об этом акт, подписываемый комиссией, назначенной приказом руководителя ОУ.

Для облегчения контроля все документы следует разделить на две группы: для общего пользования и для служебного пользования (ограниченного пользования).

Документам каждой категории необходимо присвоить свой гриф. Это можно сделать при помощи штампов, специальных отметок или цветового выделения (для общего пользования – зеленый цвет, для служебного – красный).

При присвоении соответствующего грифа соблюдаются определенные правила, которые необходимо учитывать в своей работе:

- ответственность за присвоение соответствующего грифа несет исполнитель документа, а субъектом оценки его присвоения является руководитель ОУ;
- ценность информации определяется с помощью таких критериев, как полезность, своевременность, актуальность, достоверность, конфиденциальность;
- информация подлежит защите при условии, что доступ к ней закрыт на законном основании.

В ходе использования, передачи, копирования и исполнения документов также необходимо соблюдать определенные правила:

1. Все документы, независимо от грифа, передаются исполнителю под роспись в журнале учета документов.
2. Документы, дела и издания с грифом "Для служебного пользования" ("Ограниченного пользования") должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах. При этом должны быть созданы условия, обеспечивающие их физическую сохранность.
3. Выданные для работы дела и документы с грифом "Для служебного пользования" ("Ограниченного пользования") подлежат возврату в канцелярию в тот же день.
4. Передача документов исполнителю производится только через канцелярию или ответственного за организацию делопроизводства.
5. Запрещается выносить документы с грифом "Для служебного пользования" за пределы ОУ.
6. При смене работников, ответственных за учет и хранение документов, дел и изданий, составляется по произвольной форме акт приема-передачи документов.

Для организации делопроизводства приказом руководителя ОУ назначается ответственное лицо. Делопроизводство ведется на основании инструкции по организации делопроизводства, утвержденной руководителем ОУ. Контроль за порядком его ведения возлагается на ответственного за информационную безопасность.

Контроль за выполнением требований по организации делопроизводства осуществляется в целях изучения и оценки фактического состояния сохранности документов, выявления недостатков, их устранения, установления причин таких недостатков и нарушений и выработки предложений по совершенствованию системы делопроизводства.

Огромную помощь в повышении информационной безопасности может сыграть ее аудит. Проведение независимого аудита позволяет выявить уязвимые места, возможные каналы утечки информации, объективно оценить режим информационной безопасности. Грамотно проведенный аудит информационной безопасности позволяет добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности ОУ.

Таким образом, обеспечение информационной безопасности ОУ в современных условиях становится одним из основных видов его деятельности. Без использования новых подходов, поиска современных форм и способов обеспечения безопасности ОУ решить эти задачи невозможно.

Нормативные документы

- Трудовой кодекс РФ от 30.12.2001 № 197-ФЗ (с изм. и доп.)
- Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"
- Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных"

А.А.Парфенов,
канд. воен. наук, доц. Педагогической академии последипломного образования Минобразования Московской области, чл.-корр. Международной академии наук экологии и безопасности жизнедеятельности