Защита конфиденциальной информации в условиях ВУЗа

Светлана Александровна Корягина
Компания OCS
kuzinasvetlaya@yandex.ru
0000-0003-0452-3370

Поступила в редакцию 26.04.2021
Принята 14.08.2021
Опубликована 15.09.2021

10.25726/f9834-2371-9486-f

Аннотация

Активное развитие глобальной экономической среды и национальных систем происходит в условиях интенсивного внедрения инновационных технологий. Интеграция высокотехнологичных электронных устройств в различные процессы на уровне стран, видов экономической деятельности, отдельных предприятий и в частном жизни населения приводит к генерации значительных объемов информации. Отдельное место в качестве источника генерирования данных занимает сеть Интернет, что служит инструментом создания, накопления и передачи информации. В указанных условиях информация выступает в виде ресурса, который можно оценить в денежной форме исходя из специфики данных и спроса среди отдельных групп пользователей. Отдельные государства пытаются завладеть секретной информации других стран, компании используют промышленный шпионаж для получения секретной информации конкурентов, во многих случаях фиксируются случаи похищения персональной информации граждан с целью получения определенной выгоды и тому подобное. Приведенная ситуация приводит к разработке национальных стратегий защиты в сфере информационной безопасности и активной разработки специализированных продуктов, позволяющих с помощью аппаратного и программного обеспечения минимизировать потерю информационных ресурсов стран, компаний, граждан и тому подобное. Рынок представленных продуктов активно развивается и имеет значительный потенциал для роста, поскольку происходит непрерывная эволюция методов, которые нацелены на незаконное завладение коммерческой и частной информации. В отдельных случаях главной целью незаконно доступа к информации является блокирование доступа к ней владельцев или полное уничтожение данных, что негативно влияет на функционирование компании в целом или отдельных систем. Исходя из международного опыта и ситуации в России, в первую очередь речь идет о хакерской атаке в 2017 г. через специализированное бухгалтерское программное обеспечение M.E.Doc, следует отметить активизацию государственных мероприятий, которые ориентированы на предотвращение незаконного нарушения информационной безопасности. Например, после хакерских атак в 2017 г. был создан Ситуационный центр обеспечения кибернетической безопасности. Специфика функционирования учебных заведений предусматривает генерирование персональной информации учащихся, студентов и педагогических работников, баз данных с учебными материалами, текущей документации и тому подобное. Для обеспечения эффективного функционирования учебных структур необходимо создать действенную систему защиты информации, которая позволит минимизировать риски потери или повреждения соответствующих данных.

Ключевые слова

Защита информации, функционирование, образование, управление.

Введение

В развитых странах мира современная система образования обеспечивается благодаря эффективной государственной политике регулирования ключевых процессов, разработке и реализации

действенных стратегий развития и соответствующем финансировании предусмотренных мероприятий, в том числе и в сфере внедрения инновационных технологий. В России очерченным вопросам также уделяется определенное внимание, однако существует потребность в внедрении передового опыта отдельных государств мира в сфере защиты информации в образовательных учреждениях. Следует отметить, что к образовательному процессу привлекаются дети и подростки, которые очень чувствительны к восприятию любой информации, которая может пропагандировать вредные для здоровья, психики и безопасности данной категории населения ценности (Беззубов, 2017). Наряду с этим, нужно обеспечить защиту персональных данных школьников и студентов от завладения злоумышленниками. В системе образования также хранится информация о педагогических и других категориях работников, учебные материалы в цифровом виде, финансовые и бухгалтерские данные, а также служебная документация, приведенные электронные материалы также нуждаются в защите. Для обеспечения функционирования образовательных учреждений и нормальной жизнедеятельности всех участников учебного процесса система информационной безопасности должна минимизировать риски повреждения баз данных, похищения массивов конфиденциальных сведений, а также гарантировать невозможность проникновения в учебные помещения пропаганды, которая негативно влияет на сознание учащихся и школьников (Козачок, 2012).

Информационная безопасность образовательного учреждения представляет собой сложную систему, которая предусматривает защиту имеющегося в организации информационного пространства и делает невозможным повреждение или похищение персональных данных всех участников учебного процесса, а также информации, которая позволяет учреждению функционировать и имеет денежную, образовательную, интеллектуальную ценность и тому подобное. Обеспечение эффективного функционирования системы безопасности предусматривает затраты определенных денежных ресурсов в рамках разработанной стратегии защиты данных (Стукалова, 2017).

Рассмотрим более подробно информацию, которая находится в распоряжении учебных заведений в России (Тюменев, 2018):

1. Персональные данные учащихся, студентов, преподавателей и других категорий работников. В России согласно с требованиями Конвенции Совета Европы о защите лиц в связи с автоматизированной обработкой персональных данных 1 июня 2010 г. был принят Федеральный Закон «О защите персональных данных». В соответствии с представленным нормативно-правовым актом предусматривается комплекс мер по защите частной информации и устанавливается ответственность за ее неправомерное распространение.
2. Структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, учебные программы). Защита указанной группы информации осуществляется в связи с необходимостью предотвращения ее частичного или полного повреждения, то есть минимизации рисков нарушения или полного прекращения функционирования образовательного учреждения на определенный период времени. Наряду с этим, учебная информация может содержать элементы интеллектуальной собственности, которые были разработаны работниками образовательного учреждения в рамках действующего законодательства или получены у других структур в соответствии с определенными правоотношениями. В определенных случаях образовательное учреждение использует учебную информацию только для собственных нужд и не желает предоставлять учебно-методические разработки в пользование другим учреждениям. Ограничение доступа к финансовой информации осуществляется для предотвращения махинаций с имеющимися средствами. В современных условиях внедрение систем оценок знаний учащихся и студентов за помощью специализированного программного обеспечения, важно обеспечить их объективность, что предполагает защиту представленных систем от внешнего вмешательства.
3. Научные наработки, которые наделены признаками интеллектуальной собственности и защищены законодательством. Специфика функционирования учебных учреждений, в первую очередь высших учебных заведений, предусматривает проведение преподавательским персоналом научных исследований, активного участия в грантовых программах и тому подобное. Полученные в процессе исследований научные результаты, а также сгенерированные в процессе данные, нуждаются в защите

как продукты интеллектуальной собственности (Козьминых, 2016). Особое внимание нужно уделять ограничению доступа к информации, генерируемой на этапе апробации и не получила вид комплексного научного продукта, который опубликован или запатентованный соответствующими учеными.

Материалы и методы исследования

Для обеспечения защиты информации в учебных заведениях должны быть предусмотрены денежные ресурсы на содержание персонала, имеющий соответствующий уровень квалификации. Количество специалистов в сфере IT-защиты должна отвечать специфике функционирования образовательного учреждения, особенностям имеющихся баз данных, численности персонала и обучающихся. К основным должностным обязанностям указанных работников необходимо отнести (Макаренко, 2018):

– обеспечение бесперебойной доступности к информации в целом или отдельных ее модулей в любое время для пользователей в соответствии с их правами доступа;

– создание условий защиты от полной или частичной потери информации, несанкционированного внесения изменений в данные лицами, не имеющими соответствующих полномочий;

– конфиденциальность и недоступность данных для третьих лиц.

Угрозы информационной безопасности образовательных учреждений связаны не только с деятельностью специализированных хакерских групп, действующих в собственных интересах или выполняющих заказы третьей стороны, но и связаны с непосредственными участниками учебного процесса – школьниками и студентами, которые случайно или намеренно могут испортить компьютерное оборудование, повредить или удалить определенную информацию, установить вредоносное программное обеспечение и тому подобное. Отнесение данной категории граждан к группе риска связано с психологическими особенностями, которые присущи детям и подросткам: любознательность, неосмотрительность, беззаботность, повышенное чувство справедливости и тому подобное.

Выделяются пять групп объектов, которые могут подвергнуться преднамеренному или непреднамеренному воздействию:

– компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, интеграции вредоносного программного обеспечения и т. д;

– специализированное программное обеспечение, которое используется для функционирования образовательного учреждения или непосредственно применяется в учебном процессе и может полностью или частично потери функциональность вследствие хакерских атак, активации вирусов или других вредоносных действий;

– информация учебных заведений, которая хранится на различных носителях и используется для обеспечения функционирования указанных учреждений;

– школьники и студенты, которые относятся к группе риска вследствие их уязвимости к негативному информационному воздействию, что может нанести вред им непосредственно или привести к агрессивному поведению по отношению к окружающим или учебному заведению;

– персонал учебного заведения, который под влиянием внешних факторов или по собственным мотивам может негативно повлиять на информационную безопасность учебного заведения, частично или полностью уничтожив информацию, использовав ее в личных интересах или передав данные третьим лицам.

Результаты и обсуждение

В рамках разработки эффективной стратегии информационной безопасности образовательных учреждений целесообразно выделить пять основных направлений защиты данных (Mahfuth, 2017):

1. Нормативно-правовой. Комплексная организация противодействия с незаконным завладением данными или их уничтожением базируется на действующей нормативно-правовой базе РФ. Наряду с этим существует ряд стандартов, инструкций и рекомендаций, ориентированных на обеспечение информационной безопасности, в том числе и в учебных заведениях.

2. Морально-этический. Одной из ключевых функций образовательной системы является формирование у учащихся и студентов системы моральных ценностей, которые являются положительными ориентирами в обществе. Для достижения приведенной цели учебным заведениям необходимо реализовывать комплекс мероприятий, защищающих подростков от вредной информации. Формирование у школьников и студентов системы ценностей уменьшает вероятность совершения правонарушений данной категорией населения, в том числе на территории учебных заведений.

3. Административно-организационный. Представлен направление предполагает разработку внутренних инструкций, регламентирующих особенности использования компьютерного оборудования, специфике работы с информацией и ее носителями. Кроме того, необходимо сформировать правила доступа школьников и студентов к сети Интернет в компьютерных классах, порядок блокировки опасного для данной категории населения контента, запрет на пользование собственными носителями информации. Должно быть предусмотрено использование системы родительского контроля над ресурсами сети Интернет.

4. Физический. В рамках данного направления предусматривается формирование пропускной системы согласно уровню доступа к помещениям, в которых размещаются носители информации учебного заведения. В помещение допускаются только авторизованные пользователи, а использование ими информации осуществляется строго в пределах их прав доступа к данным. Установленные пароли должны регулярно меняться с целью минимизации рисков завладения информацией третьими лицами или ее уничтожения. К мерам физической защиты может быть отнесено обязательное копирование важной информации на диски компьютеров, не имеющих доступа к сети Интернет.

5. Технический. Для обеспечения качественной защиты информации в образовательных учреждениях необходимо использовать специализированное программное обеспечение, которое дает возможность выявлять потенциальные угрозы и реализовывать меры борьбы с ними. В условиях недостаточного уровня финансирования мероприятий, которые ориентированы на обеспечение информационной безопасности образовательных учреждений, большинство учреждений использует только антивирусы и бесплатные программные продукты в сфере борьбы с незаконным нарушением информационных систем. Предполагается установка фильтров, которые ограничивают доступ школьников и студентов к определенным ресурсам в сети Интернет. Нужно установить контроль за доступом сотрудников, учеников и студентов к электронной почте. Также необходимо ввести запрет на копирование определенных видов информации с компьютеров образовательного учреждения.

Эффективная стратегия информационной безопасности предусматривает комплексное использование приведенных выше направлений защиты данных. Ключевая роль на этапе предотвращения незаконного завладения информацией отводится должностным лицам, которые непосредственно реализуют комплекс мер защиты данных. Наряду с учебными заведениями реализацию воспитательной функции в сфере информационной грамотности и безопасности учащихся и студентов должны выполнять родители (Рузов, 2018).

Эффективное функционирование высших учебных заведений в современных условиях возможно только при условии реализации комплекса мероприятий, которые ориентированы на соблюдение информационной безопасности. Интенсивное генерирование образовательными учреждениями больших объемов информации во время учебного и научного процесса предусматривает создание условий по ее надежному хранению. Эволюция вредоносного программного обеспечения для незаконного завладения данными требует от учебных учреждений осуществлять комплекс мероприятий в рамках оптимизации стратегии обеспечения информационной безопасности.

Защита информации является целенаправленной деятельностью владельцев информации, направленной на исключение или существенное ограничение возможностей утечки, навязывание, блокирования или уничтожения информации, подлежащей защите. Одним из возможных путей научного поиска в выбранном направлении является исследование защиты информации как системы, то есть как целостного образования, что интересует нас в своем единстве, причем стоит помнить, что любой объект представляет собой систему лишь относительно определенной цели.

Заметим, что в соответствии с системным подходом, примененным в научной литературе, закономерности целого (системы) безусловно доминируют над ее компонентами. Однако роль составляющих не стоит сводить к положению сугубо пассивных частей. Будучи зависимыми от системы как целого, компоненты имеют определенную относительную самостоятельность.

Нормативно-правовое понимание административно-правовых мер защиты информации, в том числе информации с ограниченным доступом, сводится к системы правовых, организационных, инженерно-технических мероприятий, которые направляются на сохранение целостности служебной информации и предотвращения ее утечки.

Система защиты может быть разной, по усмотрению владельца, а может и не иметь такой защиты вообще. Он осуществляется на основе диспозитивных методов, входящих в сферу гражданско-правого рассмотрения. Защита информации становится предметом административно-правового регулирования в случаях, когда ограничение доступа к информации прямо предусматриваются законами, когда эти ограничения связаны с обеспечением информационных прав и свобод человека, информационных аспектов национальной, государственной, общественной безопасности и тому подобное, а субъектом применения этих ограничений, что очень важно, является государство в лице его компетентных органов.

Юрисдикционные формы реализации административно-правовых мер защиты информации с ограниченным доступом у субъектов хозяйствования реализуются с целью восстановления нарушенных прав субъектов информационных правоотношений. К этим мерам относим прежде всего следующие:

- отнесение сведений к информации с ограниченным доступом;
- документирование информации по ограниченному доступу, что является основой для регистрации информационных ресурсов;
- правовая защита информации по ограниченному доступом, что выражается в существовании института административно-правовой ответственности за нарушение законодательства о служебную информацию, который является одной из гарантий надлежащей реализации и защиты.

Для высшего учебного заведения типичными категориями становятся те, которые принимают участие в жизнедеятельности заведения, существенно влияют на состояние ИБ, имеют следующие характеристики и оценки.

Заключение

Характерным признаком современного этапа научно-технического прогресса является стремительное развитие информационных технологий, их использование в повседневной жизни. Наличие и доступность высокотехнологичного оборудования, создание глобальных информационно-телекоммуникационных сетей, интеграция информационных систем научных учреждений с целью рационального использования информационного ресурса (ИР) способствуют интенсификации работы научно-педагогических и других работников Высших учебных заведений и улучшают учебный процесс, который все чаще приобретает черты дистанционного обучения.

Вместе с тем неконтролируемый доступ к информационному ресурсу высшего учебного заведения, состояние информационной безопасности (ИБ), низкая защищенность от внешних и внутренних угроз имеют негативные последствия – риск нарушения целостности, доступности и конфиденциальности информации.

Совершенствование управления информационными рисками сложная задача, которая требует глубокого исследования угроз ИБ, источниках и причин их возникновения, оценки уровня уязвимости IP учебного заведения, что в свою очередь позволит осуществить синтез модели нарушителя ИБ и в дальнейшем когнитивной модели управления рисками. Поэтому актуальность темы очевидна, поскольку система ИБ отражает состояние защищенности интересов не только студентов и преподавателей, но и национальных интересов страны, потому что последние проводят кроме обучающей еще и научную работу.

Список литературы

1. Беззубов А.Ф., Синицын И.В. Применение вычислительных систем отечественного производства как средство повышения информационной безопасности вуза // Вестник Российской таможенной академии. 2017. №(2). С. 106-110.
2. Горюнов А.Г. Внутренний аудит информационной безопасности предприятия // Вестник Московского университета МВД России. 2012. №(8). С. 227-231.
3. Козачок А.И., Левицкая Ю.А. Методы оценки информационных рисков в сетях учебного назначения // Методические вопросы преподавания инфокоммуникаций в высшей школе. 2012. № 1(4). С. 27-29.
4. Козьминых С.И., Козьминых П.С. Аудит информационной безопасности // Вестник Московского университета МВД России. 2016. № 1. С. 181-186.
5. Кузнецов В.Н. Социология безопасности: Учеб. пособ. М.: МГУ, 2007. 424 с.
6. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий // Системы управления, связи и безопасности. 2018. №1. С. 1-29.
7. Немов Р.С. Психологический словарь. М.: ВЛАДОС, 2007. 560 с.
8. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В.В. Виноградова. 4-е изд., доп. М.: А ТЕМП, 2006. 944 с.
9. Рузов А., Князьков А. Информационная безопасность курсантов военных институтов // Сб. учеб.-метод. мат-лов «Войсковой вестник». Прил. к журн. «На боевом посту». 2018. № 2. С. 57-61.
10. Ситнов А.А. Организация аудита информационной безопасности // Учет. Анализ. Аудит. 2016. № 3(6). С. 102-110.
11. Стукалова О.В., Боякова Е.В., Юдушкина О.В. Системный подход к обеспечению информационной безопасности в образовательных организациях (на примере вузов) // ВестникНЦБЖД. 2017. № 32(2). С. 104-109.
12. Тюменев А.В., Панов Н.Н. Комплексная информационная безопасность в вузе // Экстремальная деятельность человека. 2018. № 47. С. 65-68.
13. Ушаков Д.Н. Толковый словарь современного русского языка. М.: Аделант, 2014. 800 с.
14. Шабанов А.А. Предпосылки формирования системы информационной безопасности в вузах. Конкурентоспособность в глобальном мире: экономика, наука, технологии. 2017. № 5-2 (44). С. 177-180.
15. Mahfuth A., Bakar A. A., Yussof S., Ali N. A systematic literature review: Information security culture. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). DOI: 10.1109/ ICRIIS.2017.8002442

Protecting confidential information in a university environment

Svetlana A. Koryagina
OCS Company
kuzinasvetlaya@yandex.ru
0000-0003-0452-3370

Received 26.04.2021
Accepted 14.08.2021
Published 15.09.2021

10.25726/f9834-2371-9486-f

Abstract

The active development of the global economic environment and national systems takes place in the conditions of intensive introduction of innovative technologies. The integration of high-tech electronic devices into various processes at the level of countries, types of economic activity, individual enterprises and in the private life of the population leads to the generation of significant amounts of information. A separate place as a source of data generation is occupied by the Internet, which serves as a tool for creating, accumulating and transmitting information. Under these conditions, information acts as a resource that can be evaluated in monetary form based on the specifics of the data and demand among individual user groups. Individual states are trying to seize the secret information of other countries, companies use industrial espionage to obtain the secret information of competitors, in many cases, cases of theft of personal information of citizens for the purpose of obtaining a certain benefit are recorded, and so on. This situation leads to the development of national protection strategies in the field of information security and the active development of specialized products that allow using hardware and software to minimize the loss of information resources of countries, companies, citizens, and the like. The market of the presented products is actively developing and has a significant potential for growth, since there is a continuous evolution of methods that are aimed at illegal acquisition of commercial and private information. In some cases, the main purpose of illegal access to information is to block the owners ' access to it or completely destroy the data, which negatively affects the functioning of the company as a whole or individual systems. Based on international experience and the situation in Russia, first of all, we are talking about a hacker attack in 2017 through specialized accounting software M.E.Doc it should be noted the intensification of state measures that are aimed at preventing illegal violations of information security. For example, after the hacker attacks in 2017 A Situational center for Cybernetic security was created. The specifics of the functioning of educational institutions provide for the generation of personal information of students, students and teaching staff, databases with educational materials, current documentation, and the like. To ensure the effective functioning of educational structures, it is necessary to create an effective information protection system that will minimize the risks of loss or damage to the relevant data.

Keywords

Information protection, operation, education, management.

References

1. Bezzubov A.F., Sinicyn I.V. Primenenie vychislitel'nyh sistem otechestvennogo proizvodstva kak sredstvo povyshenija informacionnoj bezopasnosti vuza // Vestnik Rossijskoj tamozhennoj akademii. 2017. №(2). S. 106-110.
2. Gorjunov A.G. Vnutrennij audit informacionnoj bezopasnosti predprijatija // Vestnik Moskovskogo universiteta MVD Rossii. 2012. №(8). S. 227-231.
3. Kozachok A.I., Levickaja Ju.A. Metody ocenki informacionnyh riskov v setjah uchebnogo naznachenija // Metodicheskie voprosy prepodavanija infokommunikacij v vysshej shkole. 2012. № 1(4). S. 27-29.
4. Koz'minyh S.I., Koz'minyh P.S. Audit informacionnoj bezopasnosti // Vestnik Moskovskogo universiteta MVD Rossii. 2016. № 1. S. 181-186.
5. Kuznecov V.N. Sociologija bezopasnosti: Ucheb. posob. M.: MGU, 2007. 424 s.
6. Makarenko S.I. Audit informacionnoj bezopasnosti: osnovnye jetapy, konceptual'nye osnovy, klassifikacija meroprijatij // Sistemy upravlenija, svjazi i bezopasnosti. 2018. №1. S. 1-29.
7. Nemov R.S. Psihologicheskij slovar'. M.: VLADOS, 2007. 560 s.
8. Ozhegov S.I., Shvedova N.Ju. Tolkovyj slovar' russkogo jazyka: 80 000 slov i frazeologicheskih vyrazhenij / Rossijskaja akademija nauk. Institut russkogo jazyka im. V.V. Vinogradova. 4-e izd., dop. M.: A TEMP, 2006. 944 s.
9. Ruzov A., Knjaz'kov A. Informacionnaja bezopasnost' kursantov voennyh institutov // Sb. ucheb.-metod. mat-lov «Vojskovoj vestnik». Pril. k zhurn. «Na boevom postu». 2018. № 2. S. 57-61.

10. Sitnov A.A. Organizacija audita informacionnoj bezopasnosti // Uchet. Analiz. Audit. 2016. № 3(6). S. 102-110.

11. Stukalova O.V., Bojakova E.V., Judushkina O.V. Sistemnyj podhod k obespecheniju informacionnoj bezopasnosti v obrazovatel'nyh organizacijah (na primere vuzov) // VestnikNCBZhD. 2017. № 32(2). S. 104-109.

12. Tjumenev A.V., Panov N.N. Kompleksnaja informacionnaja bezopasnost' v vuze // Jekstremal'naja dejatel'nost' cheloveka. 2018. № 47. S. 65-68.

13. Ushakov D.N. Tolkovyj slovar' sovremennogo russkogo jazyka. M.: Adelant, 2014. 800 s.

14. Shabanov A.A. Predposylki formirovanija sistemy informacionnoj bezopasnosti v vuzah. Konkurentosposobnost' v global'nom mire: jekonomika, nauka, tehnologii. 2017. № 5-2 (44). S. 177-180.

15. Mahfuth A., Bakar A. A., Yussof S., Ali N. A systematic literature review: Information security culture. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). DOI: 10.1109/ ICRIIS.2017.8002442