• Если у вас на телефоне есть технология Bluetooth, убедитесь, что она отключена, или телефон находится в скрытом режиме. Убедитесь, что доступ к вашему телефону по Bluetooth можно получив только введя пароль. Содержание телефона с включенным Bluetooth, который не защищен паролем, может быть прочитано любым человеком с Bluetooth устройством в диапазоне действия.

• Многие ручные игровые консоли и некоторые MP3-плееры также имеют Bluetooth и могут быть использованы для установления контактов с "чужим" устройством.

Предлагаемый комплекс советов является базовым и не в состоянии охватить всех ситуаций, которые могут возникнуть у учителя в процессе использования полного спектра возможностей, предлагаемых информационно-коммуникационными технологиями, однако следование основным принципам поможет снизить риск возможных ошибок.

Список литературы

1. The Learning Resource Exchange / European Schoolnet [Электронный ресурс]. - Режим доступа: lreforschools.eun.org/web/community/.

2. London Greed for Learning [Электронный ресурс]. - Режим доступа: - www/lgfl.net/safety/pages/policies-acceptable-use//tab=4.

УДК 004.056

И.В. Гаврилова

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Гаврилова Ирина Викторовна
ipopova@masu-inform.ru
ФГАОУ ВПО «Магнитогорский государственный технический университет им. Г.И. Носова», Россия, г. Магнитогорск,

THE ORGANIZATION OF PERSONAL INFORMATION PROTECTION IN EDUCATIONAL INSTITUTIONS

Gavrilova Irina Victorovna
Russian State Technical University, Russia, Magnitogorsk

Аннотация. *В статье рассматриваются организационные аспекты обеспечения защиты* персональных данных в образовательных учреждениях согласно современному законодательству, описывается метод оценки требуемого уровня защищённости персональных данных.

Abstract*. The article deals with organizational aspects of ensuring protection of personal information in educational institutions according to the modern legislation. The method of an assessment of demanded level of security of personal information is described.*

Ключевые слова*: персональные данные; защита; образовательные учреждения.*
Keywords*: personal information; protection; educational institutions.*

Федеральный закон «О персональных данных» (№152-ФЗ) был принят 27 июля 2006 г. и с тех пор его требования к защите персональных данных (ПД) неоднократно пересматривались. Согласно положениям закона ПД является практическая любая информация, относящаяся к физическому лицу, поэтому руководство организации, по каким-либо причинам не обеспечившее их достаточную защиту, несет административную и уголовную ответственность. Колоссальный объем ПД ежедневно обрабатывается в образовательных учреждениях, поскольку их основные бизнес-процессы напрямую связаны с физическими лицами. По этой причине организация защиты ПД именно в учреждениях системы образования является первоочередной задачей.

Прежде всего, лицо, осуществляющее защиту ПД в организации, должно в обязательном порядке определить требуемый уровень защищенности информационных систем персональных данных (ИСПД). В настоящий момент выделено 15 групп различных технических и организационных мер, в каждой из которых от 2 до 20 базовых (обязательных) или компенсирующих. [1] Следует отметить, что в перечне есть немало мер, которые могут быть только компенсирующими (они не отмечены плюсом ни для одного из четырех уровней защищенности). Требуемый уровень защищенности определяется согласно Постановлению Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В нём определены три типа угроз безопасности ПД:

- угрозы 1-го типа актуальны для ИСПД, если для нее, в том числе, актуальны угрозы, связанные с наличием недокументированных возможностей в системном программном обеспечении, используемом в ИСПД;
- угрозы 2-го типа актуальны для ИСПД, если для нее актуальны угрозы, связанные с наличием недокументированных возможностей в прикладном программном обеспечении, используемом в ИСПД;
- угрозы 3-го типа актуальны для ИСПД, если для нее актуальны угрозы, не связанные с наличием недокументированных возможностей в системном и прикладном программном обеспечении, используемом в ИСПД. [2].

Уровень защищённости ПД зависит от типа угрозы, вида обрабатываемых ПД и количества записей; его можно быстро определить, пользуясь составленной автором таблицей: он находится на пересечении столбца и строки, характеризующих особенности обработки ПД в организации.

Таблица 1. Уровни защищённости ПД

Категории ПД	Типы угроз Количество записей	Угрозы 1-го типа	Угрозы 2-го типа	Угрозы 3-го типа
Специальные категории ПД	ПД сотрудников оператора или менее чем 100 тыс. субъектов ПД, не являющихся сотрудниками оператора	1	2	3
	более чем 100 тыс. субъектов ПД, не являющихся сотрудниками оператора	1	1	2

Окончание таблицы 1

Общедоступные ПД	ПД сотрудников оператора или менее чем 100 тыс. субъектов ПД, не являющихся сотрудниками оператора	2	3	4
	более чем 100 тыс. субъектов ПД, не являющихся сотрудниками оператора	2	2	4
Иные категории ПД	ПД сотрудников оператора или менее чем 100 тыс. субъектов ПД, не являющихся сотрудниками оператора	1	3	4
	Более чем 100 тыс. субъектов ПД, не являющихся сотрудниками оператора	1	2	3
Биометрические данные	-	1	2	3

Специальные категории ПД касаются расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта ПД. Биометрические ПД – сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность. Общедоступные ПД находятся в общедоступных источниках ПД (к ним относятся справочники, адресные книги, энциклопедии). [3]

Важно отметить, что в образовательных учреждениях всех уровней системы образования обрабатываются как биометрические (фотография в личном деле, студенческом билете, зачетной книжке и т.п.), так и специальные категории ПД (медицинские данные, графа «национальность» в личной карточке студента и т.п.). Это значит, что уровень защищённости ПД в образовательных учреждениях должен быть не ниже второго, обеспечение которого требует:

а) организации режима обеспечения безопасности помещений, в которых размещена ИСПД, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечения сохранности носителей ПД;

в) утверждения руководителем оператора документа, определяющего перечень лиц, доступ которых к обрабатываемым в ИСПД ПД, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использования средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

д) назначения должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе;

е) ограничения доступа к содержанию электронного журнала сообщений исключительно должностными лицами оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.[2]

Внедрение автоматизированных информационных систем, позволяющих выполнять компьютерную обработку ПД, автоматически повышает уровень защищённости ПД до первого. А это значит, что потребуется организовать автоматическую регистрацию в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПД, и создать структурное подразделение, ответственное за обеспечение безопасности ПД или возложить на одно из существующих функции по обеспечению такой безопасности.

После того, как требуемый уровень защищённости определён, необходимо выполнить анализ существующего состояния защиты ПД и определить базовый набор мер (БНМ) по обеспечению безопасности ПД для установленного уровня защищенности ПД. Иными словами, нужно выбрать из списка все меры, отмеченные плюсом для выбранного уровня защищённости.

Затем БНМ адаптируется с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы, т.е. вычеркиваются меры, которые связаны с технологиями, не используемыми в ИСПД (например, удаляются меры для защиты виртуальной инфраструктуры, если средства виртуализации не используются). В результате должен получиться список мер, который необходимо сравнить с актуальными угрозами в модели угроз: если выбранными мерами нейтрализуются не все актуальные угрозы, следует добавить в список компенсирующие меры, необходимые для нейтрализации всех оставшихся угроз.

Итоговый список мер получится только после того, как уточненный адаптированный БНМ по обеспечению безопасности ПД будет дополнен установленными в [2] и [3] мерами, которые обеспечивают выполнение требований к защите ПД. Только после этого можно приступать к действиям по защите ПД.

К сожалению, в документах, регламентирующих выполнение обозначенных выше мер, есть ряд спорных вопросов, затрагивающих обязательность привлечения к защите ПД организаций, имеющих лицензию на техническую защиту конфиденциальной информации, а также внедрения сертифицированных систем обеспечения безопасности ПД в случае их экономической нецелесообразности. Образовательные учреждения, как правило, имеют ограниченный ИТ-бюджет, который не всегда позволяет приобретение сертифицированных программных средств защиты информации. По этой причине обоснованию экономической целесообразности выбора средств защиты ПД необходимо уделять повышенное внимание.

Таким образом, защитой персональных данных в образовательных учреждениях должен заниматься отдельное должностное лицо, которое будет отслеживать требования законодательства в сфере защиты ПД и проводить соответствующие мероприятия. Любое изменение информационной инфраструктуры должно быть согласовано с ним для того, чтобы он мог оценить изменение угроз безопасности ПД и внести в систему защиты ПД требуемые корерктивы.

Список литературы

1. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://fstec.ru/component/attachments/download/562.

2. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 г. "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2012/11/07/pers-dannye-dok.html.

3. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 23.07.2013) "О персональных данных" [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_149747/?frame=5.

УДК 004+378

Е.Д. Димов

ОБУЧЕНИЕ СТУДЕНТОВ ТЕХНОЛОГИЯМ ЗАЩИТЫ ИНФОРМАЦИИ

Димов Евгений Дмитриевич
eddimov@gmail.com
Компания Jet Infosystems
г. Москва, Россия

TRAINING OF STUDENTS IN TECHNOLOGIES OF INFORMATION SECURITY

Dimov Evgeny Dmitriyevich
Jet Infosystems company
Moscow, Russia

Аннотация. *В докладе обсуждаются психологические аспекты обучения студентов технологиям защиты информации.*

Abstract*. In the report psychological aspects of training of students to technologies of information security are discussed.*

Ключевые слова*: технологии защиты информации, информационная безопасность, студент.*

Keywords: technologies of information security, information security, student.

В современных условиях повышения возможностей нанесения ущерба, связанного с хищением информации, ее уничтожением, незаконным использованием и другими противоправными действиями теория защиты информации интенсивно развивается (см., например, [1, 3, 4]). Методическая система обучения студентов вузов защите информации и информационной безопасности находит свое развитие в диссертационных исследованиях М.А. Абиссовой, А.А. Алтуфьевой, Е.Н. Боярова, Е.П. Жук, П.С. Ломаско, В.П. Полякова, И.В. Сластениной, Э.В. Тановой и других ученых.

Существующие концепции в психологии ориентированы на изучение личности человека в его разнообразной деятельности. Исследованием этой проблемы занимаются специалисты различных предметных областей: А.Г. Асмолов, Г.Д. Бухарова, В.В. Давыдов, В.С. Леднев, Н.Г. Салмина, Л.М. Фридман и др. Решение учебных задач, связанных с использованием и разработкой технологий защиты информации выполняет определенные функции в учебно-воспитательном процессе. Изложим их.