Секция «Компьютерное право и информационная безопасность»

Разработка частной модели угроз информационной безопасности для КАУ ДПО «АИРО имени А.М. Топорова»

Научный руководитель – Фролов Андрей Евгеньевич

Абросова Дарья Андреевна
Студент (магистр)
Алтайский государственный университет, Физико-технический факультет, Кафедра прикладной физики, электроники и информационной безопасности, Барнаул, Россия
E-mail: dasha130398@gmail.com

В настоящее время информационные технологии охватили все отрасли. Информация стала одним из главных ресурсов. Правильное распоряжение информацией имеет ключевое значение для развития организации и снижения уровня разнообразных рисков. Поэтому актуальной проблемой для предприятия становится обеспечение информационной безопасности (ИБ).

ИБ достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств [1].

Для определения уровня защищенности необходимо установить категории, обрабатываемых персональных данных (ПДн) субъектов (физических лиц), вид обработки по форме отношений между субъектами и организацией, количество субъектов, а также тип угроз, актуальных для информационной системы (ИС).

В зависимости от уровня защищенности ПДн определяется перечень требований, выполнение которых необходимо для нейтрализации угроз безопасности (УБ) ПДн [3].

В ходе выполнения данной работы был выполнен ряд мероприятий для обеспечения ИБ КАУ ДПО «АИРО имени Торопова»:

- определены конфигурации компьютеров, ноутбуков и ключевого оборудования сети, собраны данные о программном обеспечении компьютеров и ноутбуков института;
- определены объекты защиты и применяемые средства защиты информации (СЗИ);
- экспертным методом в соответствии с [2] определены уровень исходной защищенности ИСПДн и вероятность реализации УБПДн;
- экспертным методом на основании опроса экспертов с учетом результатов обследования ИСПДн проведено определение опасности УБПДн;
- в соответствии с правилами отнесения угрозы безопасности к актуальной для ИСПДн экспертным методом в соответствии с [2] построена модель угроз ПДн. Полученные данные приведены на рис. 1.

Источники и литература

1) ГОСТ Р ИСО/МЭК 27002–2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

2) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах. – М.: ФСТЭК России, 2008. – 10 с.

3) Как классифицировать информационную систему персональных данных: http://ispdn.ru/basis/522/

Иллюстрации

Обозначение угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y1)	Опасность угрозы	Актуальность угрозы
Внедрение в систему вредоносных программ	5	0,5	Средняя	Актуальна
Хищение элементов компьютера в составе системы, содержащих ПДн	2	0,35	Средняя	Актуальна
Хищение отчуждаемых носителей информации, содержащих ПДн	2	0,35	Средняя	Актуальна
Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа	2	0,35	Средняя	Актуальна
Внедрение по сети вредоносных программ	2	0,35	Средняя	Актуальна
Ошибочные действия пользователей, приводящие к нарушению безопасности ПДн	2	0,35	Средняя	Актуальна
Просмотр информации на дисплее серверных компонентов системы посторонними лицами, находящимися в помещении, в котором ведется обработка ПДн	10	0,25	Высокая	Актуальна
Перехват управления загрузкой операционной системы (ОС) серверных компонентов системы (угрозы, направленные на перехват паролей или идентификаторов, модификацию базовой системы ввода/вывод, перехват управления загрузкой)	2	0,35	Средняя	Актуальна
Вызов штатных программ ОС серверных компонентов системы или запуск специально разработанных программ, реализующих несанкционированный доступ к системе	2	0,35	Средняя	Актуальна

Рис. 1. Модель угроз