ОПРЕДЕЛЕНИЕ УГРОЗ И КЛАСС ЗАЩИЩЕННОСТИ ПРЕДПРИЯТИЯ

DEFINITION OF THREATS AND CLASS OF PROTECTION OF THE ENTERPRISE

УДК 004.056

Дворников Сергей Викторович, магистрант, Донской государственный технический университет, г. Ростов-на-Дону

Dvornikov S.V. sergey.dv520@gmail.com

Аннотация

Защита персональных данных в предприятиях актуальный вопрос с ростом сети Интернет и угроз для данных. Хранение и обработка персональных данных регламентируется законом. В работе рассмотрены возможные типы и классификация угроз, а также определен класс защищенности предприятия. Даны рекомендации по защите информации.

Annotation

The protection of personal data in enterprises is an urgent issue with the growth of the Internet and threats to data. The storage and processing of personal data is regulated by law. The paper considers possible types and classification of threats, and also defines the class of enterprise security. Recommendations for information protection are given.

Ключевые слова: угроза информации, несанкционированный доступ, классы, персональные данные, защита информации.

Key words: information threat, unauthorized access, classes, personal data, information protection.

Современный мир – это мир товарно-денежных отношений. Ими пронизана внутренняя жизнь любого государства. Товарные отношения достигают огромных размеров, и работать с таким количеством данных рационально на компьютерных системах. Это позволяет быстрее и удобнее оперировать необходимой информацией. Но помимо общих данных, нужно хранить персональные данные клиентов. Для того чтобы правильно хранить и оперировать персональными данными (ПДн), а также обеспечить их безопасность будем использовать Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных" [1] и Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" [2]. Также целесообразным будет использование для защиты персональных данных специализированных средств защиты.

Прежде чем определять класс защищенности предприятия необходимо рассмотреть угрозы информации для данного предприятия.

Виды и источники угроз для рассматриваемого предприятия:

1. Устаревшее программное обеспечение. 1С: Предприятие не обновлено до последней версии. С антивирусом также не известно как часто его обновляет системный администратор предприятия.

2. Учетные записи пользователя. Существует очень высокая вероятность кражи базы данных клиентов предприятия. Так как не установлены пароли при входе в систему, в которой хранятся все ПДн, и нет разграничения доступа.

3. Ошибки пользователей. От этого никто не застрахован, всегда существует человеческий фактор. Полностью исключить ее практически не возможно.

4. Ошибки в работе ПО. Для того чтобы не происходили сбои и ошибки в работе ПО необходимо обновлять его. Также с каждым обновлением разработчики убирают какие – либо уязвимости в программе, что предотвращает взлом и атаку злоумышленника.

5. Нарушение сотрудниками компании регламентов по работе с информацией. С теми сотрудниками, которые допускаются к работе с персональными данными (ПДн), необходимо проводить беседы и мероприятия по обеспечению защиты ПДн.

6. Несанкционированный доступ (НСД) к информации со стороны заинтересованных организаций и отдельных лиц. Сюда может относится промышленный шпионаж конкурентов, атаки хакеров и т.п.

7. Компьютерные вирусы и иные вредоносные программы. Могут парализовать работу предприятия на неопределенное время, что невыгодно для компании. Более часто встречающиеся вредоносные программы – это трояны, вымогатели, руткиты и т.д. Вымогатели или как еще называются «шифровальщики» атакуют компьютер и требуют выкуп за восстановление зашифрованных файлов. Шпионские программы – это программы, которые следят за деятельностью пользователя и крадут личную информацию. Клавиатурные шпионы: считывают всю информацию, которая вводится с клавиатуры. Backdoor трояны: оставляют в системе проходы (дыры), чтобы войти в компьютерную систему.

8. Стихийные бедствия и техногенные катастрофы. С точки зрения защиты ПДн необходимо недалеко от серверной хранить огнетушитель, чтобы в случае возгорания сразу же им воспользоваться, тем самым предотвратив порчу серверного оборудования и потери информации. От наводнений, землетрясений и прочего защититься должным образом не всегда получается.

9. Уничтожение информации, как случайное (стихийные бедствия, сбои, ошибки), так и специальное (злоумышленные действия людей);

Классы каналов несанкционированного получения информации могут зависеть от того, с какими элементами объекта обработки информации взаимодействовал злоумышленник. А именно [3]:

1) каналы от источника информации при НСД к нему:

– кража носителей информации;

– копирование информации;

– подслушивание разговоров, также и аудиозапись;

– установка в помещении закладных устройств и съем информации с их помощью;

– выведывание информации обслуживающего персонала;

– фотографирование или видеосъемка информации внутри помещения.

2) каналы со средств обработки информации при НСД к ним:

– снятие информации с устройств памяти;

– установка закладных устройств в средства обработки информации;

– ввод программных продуктов, позволяющих злоумышленнику получать информацию;

– копирование информации с технических устройств отображения.

3) каналы от источника информация без НСД

– получение информации по акустическим и виброакустическим каналам;

– использование технических средств оптической разведки;

– осмотр отходов и мусора;

– выведывание информации у сотрудников за пределами объекта;

4) каналы со средств обработки без НСД к ним:

– электромагнитные излучения средств обработки информации и излучения линий связи;

– подключений к линиям связи;

– снятие наводок электрических сигналов, а также с системы питания, заземления и теплоснабжения;

– подключение к базам данных по компьютерным сетям.

Потенциально возможные действия злоумышленника:

1) кража документов в бумажном и/или электронном виде, а также кража носителей информации;

2) копирование информации с носителей;

3) подслушивание разговоров и/или аудиозапись;

4) ксерокопирование, фотографирование или видеосъемка;

5) кратковременное проникновение в помещение, с целью установки прослушивающих устройств, кражи или ксерокопии документов;

6) прослушивание помещения;

7) внедрение своих людей в состав персонала конкурирующей фирмы.

Чтобы определить класс (уровень) защиты ПДн для данного предприятия воспользуемся Постановлением Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (рисунок 2).

Сначала необходимо определить категорию обрабатываемых ПДн.

Существует 4 категории ПДн [2]:

1) специальные категории ПДн, к которым относятся информация о национальной и расовой принадлежности субъекта, о религиозных, философских либо политических убеждениях, информацию о здоровье и интимной жизни субъекта;

2) биометрические ПДн, то есть данные, характеризующие биологические или физиологические особенности субъекта, например, фотография или отпечатки пальцев;

3) общедоступные ПДн, то есть сведения о субъекте, полный и неограниченный доступ к которым предоставлен самим субъектом;

4) иные категории ПДн, не представленные в трех предыдущих группах.

По форме отношений между вашей организацией и субъектами обработки подразделяются на 2 вида:

– обработка ПДН работников (субъектов, с которыми ваша организация связана трудовыми отношениями);

– обработка ПДн субъектов, не являющихся работниками вашей организации.

По количеству субъектов, ПДн которых обрабатываются, нормативным актом определены лишь 2 категории:

– менее 100 000 субъектов;

– более 100 000 субъектов;

Типы актуальных угроз:

– угрозы 1-го типа связанны с наличием недекларированных (недокументированных) возможностей в системном ПО, используемом в информационной системе персональных данных (ИСПДн);

– угрозы 2-го типа связанны с наличием недекларированных возможностей в прикладном ПО, используемом в ИСПДн;

– угрозы 3-го типа не связаны с наличием недекларированных возможностей в программном обеспечении, используемом в ИСПДн.

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Рисунок 2 – определение уровня защиты ПДн.

Для данного предприятия подходит 4 уровень защиты, так как:

– обрабатываются ПДн, относящиеся к категории «иные»;

– обрабатываются ПДн субъектов, не являющихся работниками данной организации;

– количество субъектов ПДн, которые обрабатываются в организации, не превышает 100 000 субъектов;

Для предприятия актуален 3 тип актуальных угроз.

Увеличение защищенности объекта защиты.

Требования к защите информации

– защита информации должна быть адекватной уровню важности и секретности защищаемой на предприятии информации;

– стоимость защиты не должна превышать возможный ущерб при нарушении целостности, конфиденциальности и доступности информации;

– нарушение защиты должно быть экономически не выгодно злоумышленнику, по сравнению с возможной выгодой от получения информации или ее удалении, модификации и прочего;

– защита не может быть однократной, она должна быть постоянной и непрерывной;

– защита должна быть комплексной.

Факторы, влияющие на требуемый уровень защиты информации.

Требуемый уровень защиты информации на каком – либо предприятии зависит от множества условий и факторов [4], а именно:

– от степени секретности обрабатываемой информации;

– от объема и масштаба обрабатываемой информации;

– от скорости и количеству обработки данных;

– от размера архитектуры и территориальной распределённости;

– от уровня подготовки и воспитания кадров;

– от уровня дисциплины и проводимых мероприятий по защите информации.

На компьютерах установлена операционная система windows 10, приобретена лицензия. Главное вовремя обновлять и проблем не будет.

Далее 1С: Предприятие следует установить последнее обновление, так как лицензия есть больше нечего не требуется.

На компьютерах данного предприятия установлен бесплатный антивирус Avast. Целесообразнее и надежнее было бы установить лицензионный антивирус Касперского для корпоративной сети, например, «Kaspersky Endpoint Security для бизнеса стандартный». С его помощью можно обеспечить надежную защиту.

Он позволяет защититься от криптомайнеров, усилить защиту всех узлов сети для снижения риска атак, имеет удобные инструменты контроля, также есть возможность обеспечить защиту различным ОС и т.д.

Далее необходимо настроить локальную политику безопасности, настроить разграничение доступа, установить пароли на учетные записи, удалить все не нужные программы, и запретить их свободную установку. Пароли следует менять раз в 3 месяца.

Далее, чтобы обезопасить себя от потери данных, необходимо настроить автоматическое резервное копирование данных. В программе 1С есть такая возможность и пренебрегать ей не стоит. Также есть возможность сохранять копии на внешнем жестком диске, а также возможно использование сервиса «1С Облачный архив».

При эксплуатации любого серверного и телекоммуникационного оборудования целесообразно применять системы резервного электроснабжения, наиболее часто организуемой на основе источников бесперебойного питания, его необходимо подключить к компьютеру выполняющего роль сервера, чтобы избежать непредвиденной потери данных.

Также можно настроить систему мониторинга. Она позволяет досконально знать, что делают ваша сеть, сервера и рабочие станции, также предоставит информацию для выявления и анализа проблем. Это даст возможность отслеживать в каком состоянии техника и сеть и контролировать работу сотрудников. Вот пример нескольких из них: Zabbix, Observium, Nagios.

В данной работе было рассмотрено предприятие, в котором были проведены мероприятия для повышения защиты ПДн.

Следуя рекомендациям, уровень защищенности ПДн клиентов возрастет – это позволит сохранить информацию и избежать ненужных проблем.

Литература

1. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ – Москва : Эксмо, 2019. – 32 с. (законы и кодексы).

2. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» – [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/
3. «Классы каналов несанкционированного получения информации» – [Электронный ресурс]. – Режим доступа: https://lektsii.org/5-79462.html
4. «Факторы, влияющие на требуемый уровень защиты» – [Электронный ресурс]. – Режим доступа: https://studfile.net/preview/3657038/page:2/

Literature

1. Federal Law "On Personal Data" of July 27, 2006 N 152-FZ - Moscow: Eksmo, 2019. - 32 p. (laws and codes).
2. Decree of the Government of the Russian Federation of 01.11.2012 N 1119 "On approval of requirements for the protection of personal data when processing them in personal data information systems" - [Electronic resource]. - Access mode: http://www.consultant.ru/document/cons_doc_LAW_137356/
3. "Classes of channels for unauthorized obtaining of information" - [Electronic resource]. - Access mode: https://lektsii.org/5-79462.html
4. "Factors affecting the required level of protection" - [Electronic resource]. - Access mode: https://studfile.net/preview/3657038/page:2/