# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОРПОРАЦИЙ НА ПРИМЕРЕ ПРЕДПРИЯТИЙ АВТОПРОМА

***Сорокин Никита Дмитриевич***

*В статье раскрывается сущность корпоративной безопасности, снабжения защиты информации, находящейся в информационной системе автосалона. Рассматриваются модели угроз информации и дается обобщенная характеристика информационной системы как объектов защиты. Приводится порядок и эффективность защиты информации в корпоративной сети при вводе её в эксплуатацию.*

*Ключевые слова: корпоративная безопасность, уровни, информационные ресурсы, компьютеры, информационные системы.*

*JEL-коды: J 280, L 860, L 150*

## Постановка проблемы

Проблема защиты информации является многоплановой и комплексной и охватывает ряд важных задач. Проблемы информационной безопасности постоянно усугубляются процессами проникновения во все сферы общества технических средств обработки и передачи данных и, прежде всего, вычислительных систем.

Цель статьи – проанализировать информационную безопасность корпораций на примере предприятий автопрома.

## Информационная безопасность и угрозы

Информационные ресурсы – отдельные виды документов и отдельные массивы документов, находящихся в информационных системах. Информационные ресурсы ограниченного распространения автосалонов являются элементом состава имущества и объектом права собственности. Для эффективного использования этих информационных ресурсов они должны быть надежно защищены от угроз несанкционированного распространения информации, несанкционированных и непреднамеренных воздействий на нее, которые могут привести к ее уничтожению, искажению, блокированию доступа к информации для законных пользователей[1].

Наибольшую опасность такие угрозы представляют для информации, содержащейся в персональных компьютерах, локальных и распределенных вычислительных сетях и представленных в виде носителей на магнитной и оптической основе, информативных физических полях, информационных массивах и базах данных.

Для снабжения защиты информации, находящейся в информационной системе, автосалоном ставится структурное подразделение или служебное лицо, несущие поручительство за сохранность.

В модели угроз автосалона дается обобщенная характеристика информационной системы как объектов защиты, возможных источников угрозы безопасности данных,

[1] Корпоративная безопасность [Электронный ресурс]. URL: http://www.nk-e.ru/archives/2503

основных классов уязвимостей информационных систем, возможных типов разрушительных воздействий на данные, а также основных способов их реализации.

В содержании модели угроз безопасности должны присутствовать следующие компоненты.

1. описание информационной системы и её структурно-функциональных характеристик;
2. описание угроз безопасности информации:
   - потенциал нарушителей (модель нарушителя).
   - вероятных слабостей информационной системы.
   - последствий от нарушения свойств безопасности информации.
   - способов реализации угроз безопасности информации

Сохранность информации, находящейся в информационной системе, является комбинированной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях ее создания и в процессе эксплуатации путем принятия организационно-технических мер защиты информации, направленных на блокирование угроз безопасности информации в информационной системе, в рамках системы защиты информации информационной системы автосалона (рис. 1)[2].

Работы направлены на исключение: неправомерного доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации); неправомерных уничтожения или модифицирования информации (обеспечение целостности информации); неправомерного блокирования информации (обеспечение доступности информации) организационные и технические меры защиты информации, устраиваемые в рамках системы защиты информации информационной системы, зависящие от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой.


Рис. 1. Общее требования к защите информации в информационной системе. *Источник:* составлено автором.

[2] Ковалев В. В. Корпоративные финансы и учет. Понятия, алгоритмы, показатели. - М.: Проспект, 2017. – С.114.

Порядок защиты информации в корпоративной сети при вводе её в эксплуатацию состоит из 6 основных этапов:

Первый этап – формирование требований к защите информации, содержащейся в сети. На данном этапе должны быть сгенерированы требования для определённой информационной системы. Это один из самых важных этапов, так как невозможно начать защиту информации по причине непонимания слабых и сильных сторон.

Второй этап – разработка комплексной системы защиты информации (КСЗИ). На этом этапе происходит разработка комплексной системы защиты информации.

Третий этап – внедрение КСЗИ. На текущем этапе исполнитель выполняет все без исключения пусконаладочные работы, инструктирует и обучает персонал Клиента правилам и системам эксплуатации КСЗИ. Уже после осуществлении данного этапа внедренная КСЗИ готова к дальнейшей проверке.

Четвёртый этап – аттестация информационной системы и ввод её в эксплуатацию. На данной стадии Контролирующий аппарат устанавливает Организатора государственной экспертизы, который выполняет независимое исследование соответствия КСЗИ условиям, описанным в документе «Техническое задание на создание КСЗИ», нормативной документации согласно технической защите информации, а кроме того устанавливает вероятность внедрения КСЗИ в промышленную эксплуатацию. Аттестат считается обязательным для ввода КСЗИ в промышленное использование.

Пятый этап – обеспечение защиты информации в ходе эксплуатации аттестационной информационной системы. На данной стадии Исполнитель может осуществлять авторский контроль и оказывать консалтинговую поддержку Заказчику в эксплуатации КСЗИ, анализ ее деятельности, выработку рекомендаций и, при необходимости, ее модернизации и развития.

Шестой этап – обеспечение защиты информации при выводе из эксплуатации аттестационной информационной системы или после принятия решения об окончании обработки информации. На этом этапе Заказчик обеспечивает защиту информации при окончании жизненного цикла информационной системы. Также этот этап начинает работать, когда Заказчик принимает решение об окончании обработки информации[3].

Таким образом, в автосалонах имеется информационная система, где хранится вся её информация, а именно: информация, которая приносит прибыль, персональные данные работников, персональные данные клиентов и т.п. На эту информационную систему могут нападать с целью узнать, уничтожить или изменить информацию, хранящуюся в ней.

Проведем оценку состояния безопасности корпоративной информационной системы автосалона официального дилера Renault.

Важнейшим условием реализации целей деятельности ООО «Renault» (далее Оператор) является обеспечение необходимого и достаточного уровня информационной безопасности информации, к которой, в том числе, относятся персональные данные.

Проанализировав состояние системы с точки зрения безопасности информации, можно сделать вывод, что информационная система может быть в одном из 4 состояний:

1. высокая безопасность информации – информация в безопасности;

2. средняя безопасность информации – информация в относительной безопасности, что может принести за собой среднюю степень возможного ущерба;

---

[3] Романенко О. Корпоративный контроль: трансформация, стратегия, финансы. - Saarbrücken: Lambert Academic Publishing, 2016.

3. низкая безопасность информации – информация вне безопасности, что может принести за собой высокую степень возможного ущерба;

4. очень низкая безопасность информации – информация не защищена, что может принести за собой очень высокую степень возможного ущерба.

В результате анализа информации по видам угроз безопасности информации в корпоративных информационных системах автосалона стало ясно, что потенциально самым опасным стоит считать следующих внутренних нарушителей:

1. лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступа к данным;

2. зарегистрированный пользователь с правами администратора безопасности информационной корпоративной системы Автосалона;

3. зарегистрированный пользователь информационных ресурсов, имеющий ограниченные права доступа к данным информационной корпоративной системе автосалона с рабочего места;

4. зарегистрированный пользователь с полномочиями системного администратора, т.к. вычислить их сложнее, и они имеют одноразовый или постоянный доступ к информационной системе автосалона.

Также автором были сформированы рекомендации по защите информации в информационных системах, а именно[4]:

1. Аутентификация и идентификация пользователей, которые являются работниками, операторами, обнаружение (устранение) проникновений, контроль (анализ) безопасности информации.

2. Воплощение требующихся способов (дискреционный, ролевой, мандатный либо другой способ), типов (выполнение, чтение, запись либо другой вид) и правил разделения доступа.

3. Ограничение неудачных попыток входа в информационную систему (допуска к информативной системе).

4. Урезка числа синхронных сеансов доступа для всех учетных записей пользователя информационной системы.

5. Урегулирование допуска к машинным носителям данных.

6. Ликвидации возможностей запрещенного изучения содержания данных, хранящихся на машинных носителях, и (либо) применения носителей данных в других информационных системах

7. Осуществление противовирусной охраны.

8. Обновление базы данных признаков вредных компьютерных программ (вирусов).

9. Возможность гарантировать восстановление программного обеспечения, в том числе программное обеспечение средств защиты данных, при появлении внештатных ситуаций.

10. Организация регулируемой зоны, в границах которой регулярно размещаются стационарные технические средства, обрабатывающие данные, и ресурсы защиты данных, а кроме того средства обеспечения функционирования.

11. Наблюдение и контроль за физическим доступом к техническим средствам, средствам для охраны данных, средствам обеспечения эксплуатации, в т.ч. сооружений и помещений, в которых они установлены, исключающие запрещенный физический доступ к

[4] Корпоративная безопасность [Электронный источник]. URL: http://www.nk-e.ru/archives/2503

средствам обработки данных, средствам охраны данных и средствам предоставления функционирования информационной системы, сооружения и помещения, в которых они установлены.

Таким способом, охрана данных в автомобильном салоне является эффективной в случае, если принимаемые меры отвечают определенным условиям и общепризнанным меркам.

При анализе политики информационной безопасности автосалона ООО «Автоцентр Максимум» (официальный дилер Mitsubishi), были полученные следующие результаты.

Несоответствие принимаемых мер определенным условиям и нормам по охране информации в автомобильном салоне считается патологией. Патологии согласно уровня угрозы разделяются на 2 группы:

1. неисполнение условий либо норм по охране данных в автомобильном салоне, вследствие чего имелась либо существует реальная вероятность утечки данных в автомобильном салоне узкого доступа, произошел распад, ликвидация, изменение, блокировка значимых данных в автомобильном салоне, перебои в работе средств её обработки либо существует вероятность появления этих последствий;

2. неисполнение условий либо норм по охране информации в автомобильном салоне, вследствие чего формируются посылы к утечке данных в автомобильном салоне, разламыванию, ликвидации, искривлению, блокированию значимой информации в автомобильном салоне либо к перебоям в работе средств её обработки.

По мнению С.Б.Зайнуллина, «данное несовпадение интересов может привести к конфликту между каким-либо элементом внутренней и внешней среды с корпорацией, а также к конфликту между самими элементами внутренней или внешней среды»[5].

При обнаружении патологий первой группы пользователи данных в автомобильном салоне должны:

- немедленно остановить деятельность на трудовом участке, где выявлены патологии, и осуществить мероприятия по их устранению;
- информировать отделение электронно-информационного обеспечения и охраны информации в автомобильном салоне по охране информации в автомобильном салоне об обнаружении патологии;
- организовать в определенном режиме расследование факторов и обстоятельств возникновения патологий.

Возобновление работ допускается уже после ликвидации патологий и контроля достаточности и производительности установленных мер, проводимой отделом электронно-информационного обеспечения и охраны информации в автомобильном салоне администрации.

При обнаружении нарушений второй категории отдел электронно-информационного обеспечения и защиты информации в автосалоне обязан принять необходимые меры по их устранению.

Главный вывод, который можно сделать на основании результатов исследования, заключается в том, что несмотря на более прагматичный и точечный подход российских компаний автопрома к обеспечению информационной безопасности своей IT-инфраструктуры, количество успешных атак на бизнес продолжает расти. В целом компании

5 Необходимость комплексного подхода к разрешению корпоративных конфликтов [Электронный источник]. URL: http://naukovedenie.ru/PDF/32EVN316.pdf

стали более глубоко вникать в суть существующих рисков информационной безопасности и адресно защищаться от конкретных угроз.

**Список литературы**


1. Ковалев В.В. Корпоративные финансы и учет. Понятия, алгоритмы, показатели. - М.: Проспект, 2017.
2. Колечицкий Е.С., Медведев В.Т., Кондратьева О.Е. Основы охраны труда и техники безопасности в электроустановках. - Вологда: Инфра-Инженерия, 2015.
3. Леонтьев В.Е. Корпоративные финансы. - М.: Юрайт, 2016.
4. Никитина Н.В., Янов В.В. Корпоративные финансы. - М.: КноРус, 2017.
5. Олещук Н.И., Промыслов Б.Д. Механизмы оптимизации управления деятельностью корпоративных структур. - М.: Нефть и газ, 2017.
6. Романенко О. Корпоративный контроль: трансформация, стратегия, финансы. - Saarbrücken: Lambert Academic Publishing, 2016.
7. Шаньгин В.Ф. Информационная безопасность и защита информации. - М.: ДМК, 2017.
8. Бельков Н.К. Корпоративная безопасность – защита информации компании [Электронный источник]. URL: http://office-metrika.ru/korporativnayabezopasnost.php.
9. Зайнуллин, С.Б. Необходимость комплексного подхода к разрешению корпоративных конфликтов [Электронный источник]. URL: http://naukovedenie.ru/PDF/32EVN316.pdf


# INFORMATION SECURITY OF CORPORATIONS BY THE EXAMPLE OF ENTERPRISES OF THE AUTOMOTIVE INDUSTRY


***Sorokin Nikita Dmitrievich,***

Peoples' Friendship University of Russia (RUDN University)
117198, Moscow, Miklukho-Maklaya str., 6



*The article defines the essence of corporate security, the supply of information protection, located in the information system of the showroom. Models of information threats are considered and a generalized characteristic of the information system as objects of protection is given. The order and efficiency of information protection in the corporate network is given when putting it into operation.*



*Keywords: corporate security, levels, information resources, computers, information systems.*

*JEL-codes: J 280, L 860, L 150.*