АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

ANALYSIS OF INFORMATION SECURITY THREATS AND INFORMATION LEAKAGE CHANNELS

Гринь Владислав Сергеевич, магистрант, Донской государственный технический университет, г. Ростов-на-Дону.

Grin V.S. 1voran@mail.ru

Аннотация

Работа посвящена анализу угроз информационной безопасности и каналов утечки. Составлению потенциального нарушителя.

Annotation

The work is devoted to the analysis of information security threats and leakage channels. Drawing up a potential violator.

Ключевые слова: API, социальные сети, данные, медиа файлы.

Keywords: API, social networks, data, media files.

Информационная безопасность является неотъемлемой частью любой организации. От отношения к ней напрямую зависит успех компании, так как потеря данных, это непростительный поступок, который не прощают ни инвесторы, ни клиенты. Если в организации есть собственные разработки, то их тоже необходимо защищать от атак, как внутренних, так и внешних. Для определения и последующего устранения каналов утечек информации необходимо на начальном этапе формирования компании проводить тщательный анализ уязвимостей. Это поможет как обеспечить надежность хранимых данных, так и показать организацию с лучшей стороны.

Угроза информационной безопасности представляет собой совокупность условий и факторов, создающих потенциальный или реальный риск нарушения информационной безопасности: нарушение физической целостности, логической структуры, несанкционированное изменение, получение и раскрытие информации.

По отношению к информационной системе все множество угроз можно разделить на две группы, представленные на рисунке 6.

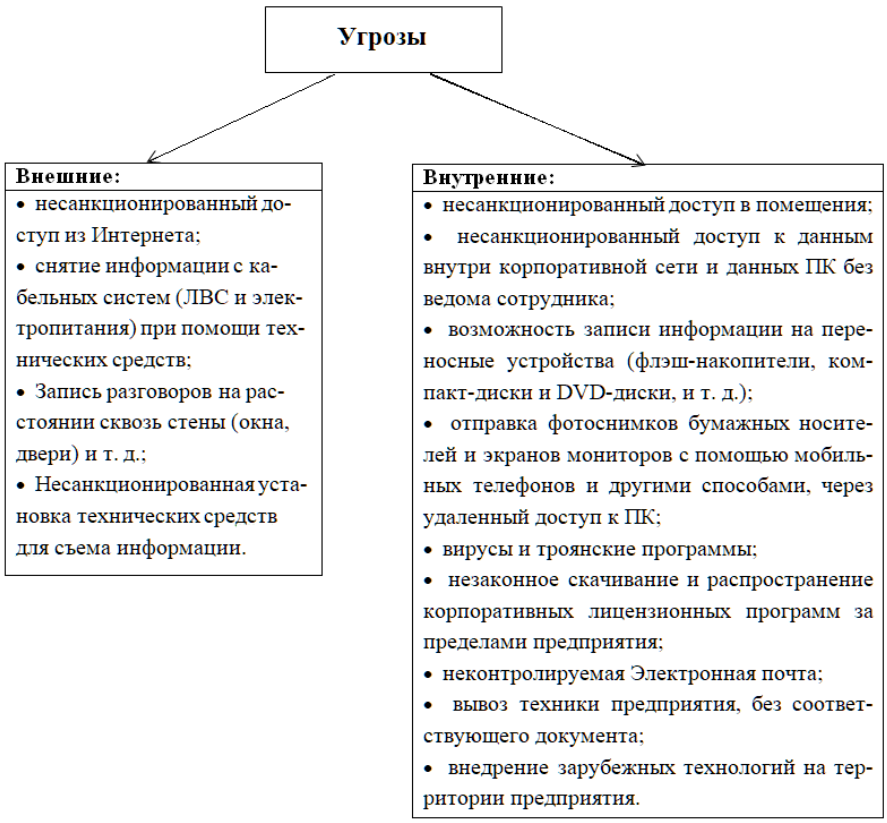


Рисунок 6 – Угрозы по отношению к информационной системе.

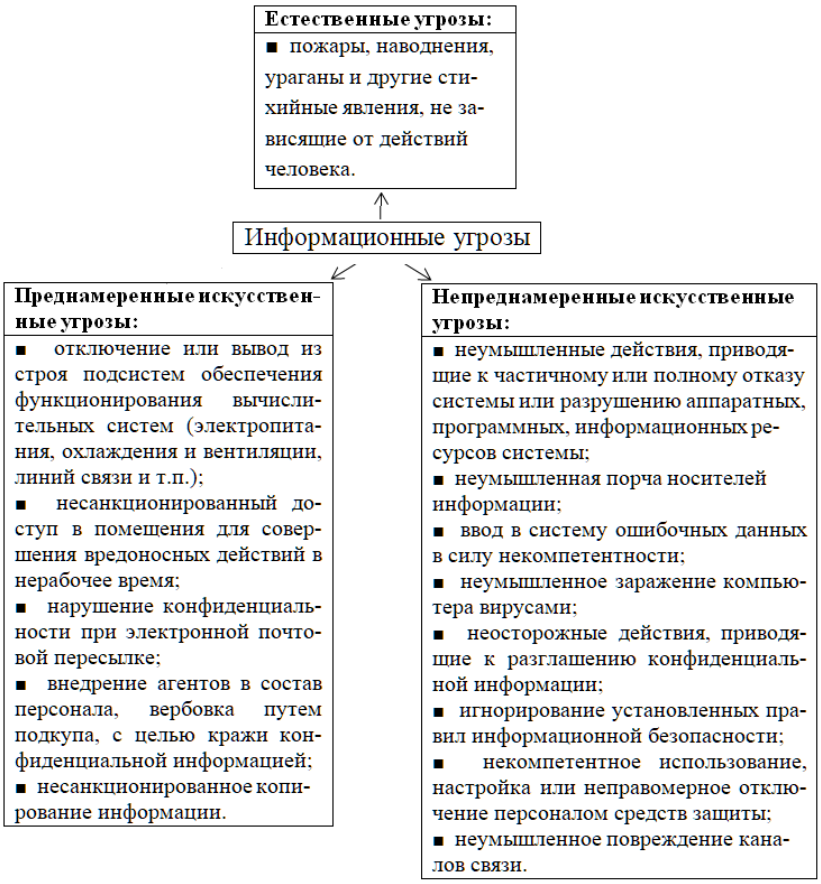


Рисунок 7 – Информационные угрозы.

Информационные угрозы подразделяются на три вида (рисунок 7).

Основными каналами НСД, при помощи которых нарушитель осуществляет хищение информации и доступ к ресурсам ИС, являются (Рисунок 8):



Рисунок 8 – Каналы утечки информации.

Составление перечня угроз и каналов утечки информации позволяет подробно проанализировать все возможные пути несанкционированного

доступа к конфиденциальной информации, и сформировать требования ксистеме защиты, следование которым обеспечит необходимый уровень защищённости информации.

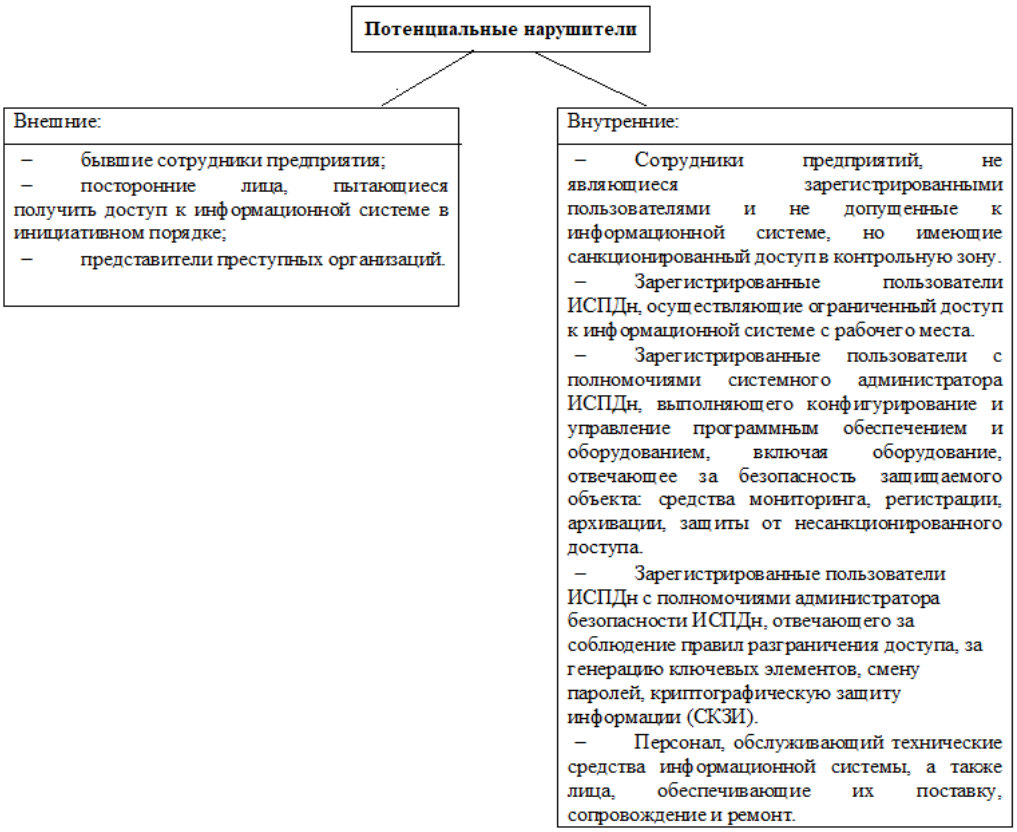


Рисунок 9 - Потенциальные нарушители.

На основании вышеизложенного, можно провести анализ “слабых” мест организации и постараться их устранить, а если это невозможно сделать, то максимально минимизировать утечку данных через каналы подобного рода.

Литература

1. Грибунин В.Г. Комплексная система защиты информации на предприятии: учебное пособие для вузов / В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
2. В. Ф. Шаньгин – «Защита информации в компьютерных системахи сетях», 2012.
3. И.В. Роберт, Т.А. Лавина – «Толковый словарь терминов понятийного аппарата информатизации образования» Москва, 2006.
4. Блюмин А.М – «Мировые информационные ресурсы», 2010.

5. Информационный Интернет-ресурс**:** it-sektor.ru.

Literature

1. Gribunin V.G. Integrated information security system at the enterprise: a textbook for universities / V.G. Gribunin, V.V. Chudovsky. - M .: Publishing Center "Academy", 2009. - 416 p.
2. VF Shangin - "Information protection in computer systems and networks", 2012.
3. I.V. Robert, T.A. Avalanche - "Explanatory dictionary of terms of the conceptual apparatus of informatization of education" Moscow, 2006.
4. Blumin AM - "World information resources", 2010.
5. Information Internet resource: it-sektor.ru.