Приложение № 3 к Политике
информационной безопасности ООО
"ЦИФРОВАЯ НЕЗАВИСИМОСТЬ"

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

1. Общие положения

Настоящий документ разработан на основе нормативно-методических документов ФСТЭК России, указанных в 4 разделе основного документа, регламентирующих порядок обеспечения безопасности коммерческой тайны.

Настоящая «Модель угроз» содержит систематизированный перечень угроз безопасности коммерческой тайны и иной защищаемой информации при их обработке в Организации. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц или организаций, а также криминальных группировок, создающими условия (предпосылки) для нарушения безопасности коммерческой тайны и иной защищаемой информации, которые ведут к ущербу жизненно важным интересам личности, общества и государства.

Модель угроз определяет актуальные угрозы для Организации.

Модель угроз содержит данные по угрозам безопасности коммерческой тайны и иной защищаемой информации, обрабатываемых в Организации, связанным:

- с перехватом (съемом) файлов, содержащих коммерческую тайну и иную защищаемую информацию, по техническим каналам с целью их копирования или неправомерного распространения;

- с несанкционированным, в том числе случайным, доступом в Организацию с целью изменения, копирования, неправомерного распространения файлов, содержащих коммерческую тайну и иную защищаемую информацию, или деструктивных воздействий на элементы Организации и обрабатываемых в ней файлов с использованием программных и

программно-аппаратных средств с целью уничтожения или блокирования файлов.

Модель угроз является методическим документом и предназначена для должностных и ответственных лиц, входящих в контакт с файлами, содержащими коммерческую тайну и иную защищаемую информацию.

Модель угроз предназначена для решения следующих задач:

- анализ защищенности Организации от угроз безопасности файлов, содержащих коммерческую тайну и иную защищаемую информацию, в ходе организации и выполнения работ по обеспечению безопасности этих файлов.

- разработка системы защиты файлов, содержащих коммерческую тайну и иную защищаемую информацию, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты, предусмотренных для соответствующего класса Организации;

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к файлам, содержащим коммерческую тайну и иную защищаемую информацию, и (или) передачи их лицам, не имеющим права доступа к такой информации;

- недопущение воздействия на технические средства Организации, в результате которого может быть нарушено их функционирование.

В Модели угроз дано обобщённое описание Организации как объекта защиты, возможных объектов воздействия угроз, модель нарушителя Организации, возможных видов неправомерных действий и деструктивных воздействий на файлы, содержащие коммерческую тайну и иную защищаемую информацию, а также основных способов их реализации.

Угрозы безопасности файлов, содержащих коммерческую тайну и иную защищаемую информацию, обрабатываемых в Организации, содержащиеся в настоящей Модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности файлов, содержащих коммерческую тайну и иную защищаемую информацию, в Организации.

2. Описание ООО “ЦИФРОВАЯ НЕЗАВИСИМОСТЬ”

2.1. Общие сведения об Организации

- Назначение Организации – создание программного обеспечения для коммерческих и государственных нужд.
- В Организации необходимо обеспечить конфиденциальность, целостность и доступность защищаемых данных.
- В Организации на регулярной обрабатывается большое количество данных, содержащих коммерческую тайну, патенты и персональные данные.

2.2. Охрана помещений

Все производство совершается в главном офисе, находящимся в бизнес центре “РТС”. Комплекс защищен охранным пунктом, ведется постоянное видеонаблюдение, установлен пропускной режим.

2.3. Используемые в Организации информационные технологии создания и использования файлов, содержащих коммерческую тайну

В Организации используются:

- Локальная сеть интернет, с поддерживаемым в ней программным обеспечением для создания и редактирования программного обеспечения;
- Система электронного документооборота;
- Бизнес решения сервисов Яндекс почта и Яндекс диск.

3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации

3.1. Описание негативных последствий и применяемых видов воздействия, актуальных для Организации, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков описано в таблице 1.

4. Возможные объекты воздействия угроз безопасности информации

4.1. Описание возможных объектов воздействия угроз, видов воздействия на компоненты систем и сетей, актуальных для Организации, описано в таблице 1.

Таблица 1. Возможные объекты воздействия угроз

№ п/п	Негативные последствия	Объекты воздействия	Виды воздействия
1.	Разглашение персональных данных граждан (У1)	База данных системы электронного документооборота	Утечка идентификационной информации граждан из базы данных
2.	Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)	Работники Организации Материальные носители информации Информационные системы Организации	Взятка, насилие, убеждение сотрудников с целью получения данных Кража, реверс инжиниринг материальных носителей информации с целью получения данных Взлом информационных систем с целью кражи, копирования, уничтожения, модификации данных
3.	Срыв запланированной сделки с партнером (У2)	Информационные системы Организации	Модификация информации и отправка её с недостоверной информацией от имени Организации и её сотрудников
4.	Саботаж текущих проектов (У2)	Работники Организации Информационные системы Организации	Взятка, насилие, убеждение сотрудников с целью саботажа проводимых проектов Взлом информационных систем с целью изменения, удаления и блокировки доступа к данным
5.	Хищение денежных средств со счета организации (У2)	Информационные системы Организации	Модификация информации и отправка её с недостоверной информацией от имени Организации и её сотрудников
6.	Изменение продукта, предназначенного для государственной структуры с целью шпионажа или саботажа (У3)	Работники Организации Информационные системы Организации	Взятка, насилие, убеждение сотрудников с целью модификации продуктов, производимых организацией Взлом информационных систем с целью модификации продуктов, производимых организацией

5. Источники угроз безопасности информации

5.1. Модель нарушителя

5.1.1. Внешний нарушитель

В качестве внешнего нарушителя информационной безопасности, рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель может воздействовать на защищаемую информацию только во время ее передачи по каналам связи.

Предполагаемые внешние нарушители:

- Преступные группы (криминальные структуры)
- Специальные службы иностранных государств
- Отдельные физические лица (хакеры)
- Конкурирующие организации
- Бывшие работники (пользователи)

Соответствие предполагаемых внешних нарушителей видам риска (ущерба) и возможным негативным последствиям:

- Преступные группы (криминальные структуры)
  - Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)
  - Хищение денежных средств со счета организации (У2)
- Специальные службы иностранных государств
  - Изменение продукта, предназначенного для государственной структуры с целью шпионажа или саботажа (У3)
- Отдельные физические лица (хакеры)
  - Хищение денежных средств со счета организации (У2)
- Конкурирующие организации
  - Срыв запланированной сделки с партнером (У2)
  - Саботаж текущих проектов (У2)
- Бывшие работники (пользователи)

- Разглашение персональных данных граждан (У1)
- Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)

Уровни возможностей нарушителей по реализации угроз безопасности информации, согласно методике оценки угроз безопасности информации:

- Преступные группы (криминальные структуры) – Н2 нарушитель, обладающий базовыми повышенными возможностями
- Специальные службы иностранных государств – Н4 нарушитель, обладающий высокими возможностями
- Отдельные физические лица (хакеры) – Н1 нарушитель, обладающий базовыми возможностями
- Конкурирующие организации – Н2 нарушитель, обладающий базовыми повышенными возможностями
- Бывшие работники (пользователи) – Н1 нарушитель, обладающий базовыми возможностями

5.1.2. Внутренний нарушитель

В качестве внутреннего нарушителя информационной безопасности, рассматривается нарушитель, который обладает достаточным доступом к техническим средствам и ресурсам Организации, находящимся в пределах контролируемой зоны.

Система разграничения доступа Организации обеспечивает разграничение прав пользователей на доступ к информационным, программным, аппаратным и другим ресурсам в соответствии с принятой политикой информационной безопасности.

Внутренний нарушитель может использовать штатные средства.

Предполагаемые внутренние нарушители:

- Разработчики программных, программно-аппаратных средств
- Поставщики вычислительных услуг, услуг связи
- Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ

- Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)
- Системные администраторы и администраторы безопасности

Соответствие предполагаемых внешних нарушителей видам риска (ущерба) и возможным негативным последствиям:

- Разработчики программных, программно-аппаратных средств
  - Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)
- Поставщики вычислительных услуг, услуг связи
  - Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)
  - Хищение денежных средств со счета организации (У2)
- Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ
  - Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)
- Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)
  - Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)
- Системные администраторы и администраторы безопасности
  - Кража, копирование, уничтожение, модификация данных, содержащих коммерческую тайну (У2)

Уровни возможностей нарушителей по реализации угроз безопасности информации, согласно методике оценки угроз безопасности информации:

- Разработчики программных, программно-аппаратных средств – Н3 нарушитель, обладающий средними возможностями
- Поставщики вычислительных услуг, услуг связи – Н2 нарушитель, обладающий базовыми повышенными возможностями

- Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ – H2 нарушитель, обладающий базовыми повышенными возможностями
- Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) – H1 нарушитель, обладающий базовыми возможностями
- Системные администраторы и администраторы безопасности – H2 нарушитель, обладающий базовыми повышенными возможностями

6. Способы реализации (возникновения) угроз безопасности информации

6.1. Способы реализации, которые могут быть использованы нарушителями описаны в таблице 2.

6.2. Интерфейсы объектов воздействия, которые могут быть использованы нарушителями описаны в таблице 2.

Таблица 2. Способы реализации (возникновения) угроз безопасности информации

№ п/п	Виды нарушителей	Интерфейсы объектов воздействия	Способы реализации (возникновения) угроз
1.	Преступные группы (криминальные структуры)	Сотрудники организации, система электронного документооборота, бизнес решения Яндекс	Реализация социальной инженерии, эксплуатация известных уязвимостей
2.	Специальные службы иностранных государств	Сотрудники организации, система электронного документооборота, бизнес решения Яндекс, локальная сеть интернет	Реализация социальной инженерии, эксплуатация известных уязвимостей, прослушивание (захват) сетевого трафика, использование недостатков конфигурации и архитектуры, атака типа "человек посередине", нарушение изоляции, использование недекларированных возможностей, внедрение программных и аппаратных закладок
3.	Отдельные физические лица (хакеры)	Система электронного документооборота, бизнес решения Яндекс	Эксплуатация известных уязвимостей
4.	Конкурирующие организации	Сотрудники организации, система электронного документооборота, бизнес решения Яндекс	Реализация социальной инженерии, эксплуатация известных уязвимостей
5.	Бывшие работники (пользователи)	Сотрудники организации	Реализация социальной инженерии
6.	Разработчики программных, программно-аппаратных средств	Сотрудники организации, система электронного документооборота, бизнес решения Яндекс, локальная сеть интернет	Использование недостатков конфигурации и архитектуры, использование недекларированных возможностей, внедрение программных и аппаратных закладок
7.	Поставщики вычислительных услуг, услуг связи	Сотрудники организации, локальная сеть интернет	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции
8.	Лица, привлекаемые для установки, настройки,	Сотрудники организации, локальная сеть интернет	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции

№ п/п	Виды нарушителей	Интерфейсы объектов воздействия	Способы реализации (возникновения) угроз
	испытаний, пусконаладочных и иных видов работ		
9.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Сотрудники организации, локальная сеть интернет	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции
10.	Системные администраторы и администраторы безопасности	Сотрудники организации, система электронного документооборота, бизнес решения Яндекс, локальная сеть интернет	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции

7. Актуальные угрозы безопасности информации

7.1. Перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей.

Перечень описан в таблице 3.

Таблица 3. Перечень возможных (вероятных) угроз безопасности информации

№ п/п	Виды нарушителей	Способы реализации (возникновения) угроз	Возможные (вероятные) угрозы безопасности информации	Меры для нейтрализации угроз
1.	Преступные группы (криминальные структуры)	Реализация социальной инженерии, эксплуатация известных уязвимостей	УБИ.1 Угроза утечки информации УБИ.2 Угроза несанкционированного доступа	Приняты
2.	Специальные службы иностранных государств	Реализация социальной инженерии, эксплуатация известных уязвимостей, прослушивание (захват) сетевого трафика, использование недостатков конфигурации и архитектуры, атака типа "человек посередине", нарушение изоляции, использование недекларированных возможностей, внедрение программных и аппаратных закладок	УБИ.1 Угроза утечки информации УБИ.2 Угроза несанкционированного доступа УБИ.3 Угроза несанкционированной модификации (искажения) УБИ.4 Угроза несанкционированной подмены УБИ.5 Угроза удаления информационных ресурсов УБИ.6 Угроза отказа в обслуживании УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника УБИ.10 Угроза распространения противоправной информации УБИ.11 Угроза несанкционированного массового сбора информации	Приняты, но недостаточны
3.	Отдельные физические лица (хакеры)	Эксплуатация известных уязвимостей	УБИ.1 Угроза утечки информации УБИ.2 Угроза несанкционированного доступа	Приняты
4.	Конкурирующие организации	Реализация социальной инженерии, эксплуатация известных уязвимостей	УБИ.1 Угроза утечки информации УБИ.2 Угроза несанкционированного доступа	Приняты
5.	Бывшие работники (пользователи)	Реализация социальной инженерии	УБИ.1 Угроза утечки информации	Приняты

№ п/п	Виды нарушителей	Способы реализации (возникновения) угроз	Возможные (вероятные) угрозы безопасности информации	Меры для нейтрализации угроз
6.	Разработчики программных, программно-аппаратных средств	Использование недостатков конфигурации и архитектуры, использование недекларированных возможностей, внедрение программных и аппаратных закладок	УБИ.1 Угроза утечки информации УБИ.3 Угроза несанкционированной модификации (искажения) УБИ.4 Угроза несанкционированной подмены УБИ.6 Угроза отказа в обслуживании	Приняты, но недостаточны
7.	Поставщики вычислительных услуг, услуг связи	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции	УБИ.1 Угроза утечки информации УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника УБИ.11 Угроза несанкционированного массового сбора информации	Приняты
8.	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции	УБИ.1 Угроза утечки информации УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника УБИ.11 Угроза несанкционированного массового сбора информации	Приняты
9.	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции	УБИ.1 Угроза утечки информации УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника УБИ.11 Угроза несанкционированного массового сбора информации	Приняты

№ п/п	Виды нарушителей	Способы реализации (возникновения) угроз	Возможные (вероятные) угрозы безопасности информации	Меры для нейтрализации угроз
10.	Системные администраторы и администраторы безопасности	Прослушивание (захват) сетевого трафика, атака типа "человек посередине", нарушение изоляции	УБИ.1 Угроза утечки информации УБИ.2 Угроза несанкционированного доступа УБИ.4 Угроза несанкционированной подмены УБИ.5 Угроза удаления информационных ресурсов УБИ.9 Угроза получения информационных ресурсов из недоверенного или скомпрометированного источника УБИ.11 Угроза несанкционированного массового сбора информации	Приняты