Приложение 6
к Методике оценки угроз
безопасности информации

Возможные цели реализации угроз безопасности информации нарушителями

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Специальные службы иностранных государств	Внешний	Нанесение ущерба государству в области обеспечения обороны, безопасности и правопорядка, а также в иных отдельных областях его деятельности или секторах экономики, в том числе дискредитация или дестабилизация деятельности отдельных органов государственной власти, организаций, получение конкурентных преимуществ на уровне государства, срыв заключения международных договоров, создание внутриполитического кризиса
2	Террористические, экстремистские группировки	Внешний	Совершение террористических актов, угроза жизни граждан. Нанесение ущерба отдельным сферам деятельности или секторам экономики государства. Дестабилизация общества. Дестабилизация деятельности органов государственной власти, организаций
3	Преступные группы (криминальные структуры)	Внешний	Получение финансовой или иной материальной выгоды. Желание самореализации (подтверждение статуса)
4	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
5	Конкурирующие организации	Внешний	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды
6	Разработчики программных, программно-аппаратных средств	Внутренний	Внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки. Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
7	Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
8	Поставщики вычислительных услуг, услуг связи	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ

№ вида	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
9	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
10	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия
11	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
12	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
13	Бывшие работники (пользователи)	Внешний	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия

Указанные возможные цели реализации угроз безопасности информации подлежат конкретизации и могут дополняться другими целями в зависимости от особенностей области деятельности, в которой функционируют системы и сети.

При оценке возможностей нарушителей необходимо исходить из того, что для повышения уровня своих возможностей нарушители 1 вида могут вступать

в сговор с нарушителями 5, 6, 7, 8, 9, 10, 11, 12 видов. Нарушители 2 вида могут вступать в сговор с нарушителями 10, 11, 12 видов. Нарушители 3 вида могут вступать в сговор с нарушителями 10, 11, 12 видов. В случае принятия таких предположений цели и уровни возможностей нарушителей подлежат объединению.

Приложение 7
к Методике оценки угроз
безопасности информации

Пример оценки целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации
(для государственной информационной системы)

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	**Нанесение ущерба юридическому лицу, индивидуальному предпринимателю**	**Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности**	
Специальные службы иностранных государств	-	-	+ (дискредитация или дестабилизация деятельности органа государственной власти*)	УЗ** (нарушение функционирования государственного органа, дискредитация деятельности органа государственной власти)
Террористические, экстремистские группировки	-	-	+ (дестабилизация деятельности органов государственной власти, организаций)	УЗ (отсутствие доступа к социально значимым государственным услугам)

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Преступные группы (криминальные структуры)	+ (получение финансовой выгоды за счет кражи и продажи персональных данных граждан)	+ (получение финансовой выгоды за счет использования вычислительных мощностей серверов государственной информационной системы для майнинга криптовалюты)	+ (желание самореализоваться)	У1 (нарушение конфиденциальности персональных данных граждан) У2 (нарушение деловой репутации) У3 (организация митингов, забастовок из-за публикаций недостоверной информации)
Отдельные физические лица (хакеры)	+ (желание самореализоваться)	+ (получение финансовой выгоды за счет кражи и коммерческой тайны)	-	У1 (нарушение личной, семейной тайны, утрата чести и доброго имени) У2 (утечка коммерческой тайны; потеря клиентов)
Конкурирующие организации	-	-	-	-
Разработчики программных, программно-аппаратных средств	-	+ (передача информации о юридическом лице третьим лицам)	+ (внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки при вступлении в сговор	У2 (недополучение ожидаемой прибыли) У3 (нарушение функционирования

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
			со специальными службами иностранных государств)	государственного органа, дискредитация деятельности органа государственной власти)
Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	-	-	-	-
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.)	-	-	-	-

Виды нарушителей	Возможные цели реализации угроз безопасности информации			Соответствие целей видам риска (ущерба) и возможным негативным последствиям
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу, индивидуальному предпринимателю	Нанесение ущерба государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической, экологической сферах деятельности	
Авторизованные пользователи систем и сетей	+ (непреднамеренные, неосторожные или неквалифицированные действия)	-	-	У1 (финансовый, иной материальный ущерб физическим лицам)
Системные администраторы и администраторы безопасности	+ (месть за ранее совершенные действия)	+ (любопытство или желание самореализации)	+ (получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой)	У1 (финансовый, иной материальный ущерб физическим лицам) У2 (невозможность заключения договоров, соглашений) У3 (утечка информации ограниченного доступа)
Бывшие (уволенные) работники (пользователи)	-	-	-	-

Приложение 8
к Методике оценки угроз
безопасности информации

Уровни возможностей нарушителей
по реализации угроз безопасности информации

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н1	Нарушитель, обладающий базовыми возможностями	Имеет возможность при реализации угроз безопасности информации использовать только известные уязвимости, скрипты и инструменты. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, имеет минимальные знания механизмов их функционирования, доставки и выполнения вредоносного программного обеспечения, эксплойтов. Обладает базовыми компьютерными знаниями и навыками на уровне пользователя. Имеет возможность реализации угроз за счет физических воздействий на технические средства обработки и хранения информации, линий связи и обеспечивающие системы систем и сетей при наличии физического доступа к ним. **Таким образом, нарушители с базовыми возможностями имеют возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов**	Физическое лицо (хакер) Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем Лица, обеспечивающие функционирование систем и сетей или обеспечивающих систем (администрация, охрана, уборщики и т.д.) Авторизованные пользователи систем и сетей Бывшие работники (пользователи)

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н2	Нарушитель, обладающий базовыми повышенными возможностями	Обладает всеми возможностями нарушителей с базовыми возможностями. Имеет возможность использовать средства реализации угроз (инструменты), свободно распространяемые в сети «Интернет» и разработанные другими лицами, однако хорошо владеет этими средствами и инструментами, понимает, как они работают и может вносить изменения в их функционирование для повышения эффективности реализации угроз. Оснащен и владеет фреймворками и наборами средств, инструментов для реализации угроз безопасности информации и использования уязвимостей. Имеет навыки самостоятельного планирования и реализации сценариев угроз безопасности информации. Обладает практическими знаниями о функционировании систем и сетей, операционных систем, а также имеет знания защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. **Таким образом, нарушители с базовыми повышенными возможностями имеют возможность реализовывать угрозы, в том числе направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети «Интернет». Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей**	Преступные группы (два лица и более, действующие по единому плану) Конкурирующие организации Поставщики вычислительных услуг, услуг связи Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ Системные администраторы и администраторы безопасности
Н3	Нарушитель, обладающий средними возможностями	Обладает всеми возможностями нарушителей с базовыми повышенными возможностями. Имеет возможность приобретать информацию об уязвимостях, размещаемую на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность приобретать дорогостоящие средства и инструменты для реализации угроз, размещаемые на специализированных платных ресурсах (биржах уязвимостей). Имеет возможность самостоятельно разрабатывать средства (инструменты), необходимые для реализации угроз (атак),	Террористические, экстремистские группировки Разработчики программных, программно-аппаратных средств

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
		реализовывать угрозы с использованием данных средств. Имеет возможность получения доступа к встраиваемому программному обеспечению аппаратных платформ, системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-аппаратным средствам для проведения их анализа. Обладает знаниями и практическими навыками проведения анализа программного кода для получения информации об уязвимостях. Обладает высокими знаниями и практическими навыками о функционировании систем и сетей, операционных систем, а также имеет глубокое понимание защитных механизмов, применяемых в программном обеспечении, программно-аппаратных средствах. Имеет возможность реализовывать угрозы безопасности информации в составе группы лиц. **Таким образом, нарушители со средними возможностями имеют возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеют возможностей реализации угроз на физически изолированные сегменты систем и сетей**	

№	Уровень возможностей нарушителей	Возможности нарушителей по реализации угроз безопасности информации	Виды нарушителей
Н4	Нарушитель, обладающий высокими возможностями	Обладает всеми возможностями нарушителей со средними возможностями. Имеет возможность получения доступа к исходному коду встраиваемого программного обеспечения аппаратных платформ, системного и прикладного программного обеспечения, телекоммуникационного оборудования и других программно-аппаратных средств для получения сведений об уязвимостях «нулевого дня». Имеет возможность внедрения программных (программно-аппаратных) закладок или уязвимостей на различных этапах поставки программного обеспечения или программно-аппаратных средств. Имеет возможность создания методов и средств реализации угроз с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение. Имеет возможность реализовывать угрозы с привлечением специалистов, имеющих базовые повышенные, средние и высокие возможности. Имеет возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений. Имеет возможность долговременно и незаметно для операторов систем и сетей реализовывать угрозы безопасности информации. Обладает исключительными знаниями и практическими навыками о функционировании систем и сетей, операционных систем, аппаратном обеспечении, а также осведомлен о конкретных защитных механизмах, применяемых в программном обеспечении, программно-аппаратных средствах атакуемых систем и сетей. **Таким образом, нарушители с высокими возможностями имеют практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-аппаратных закладок, встроенных в компоненты систем и сетей**	Специальные службы иностранных государств