ID	Нарушители	Категория нарушителя	Потенциал нарушителя
1	Неустановленные внешние субъекты (физические лица)	Внешний нарушитель	с низким потенциалом
2	Бывшие работники (пользователи)	Внешний нарушитель	с низким потенциалом
5	Пользователи информационной системы	Внутренний нарушитель	с низким потенциалом

6	Администраторы информационной системы и администраторы безопасности	Внутренний нарушитель	со средним потенциалом
9	Конкурирующие организации	Внешний нарушитель	со средним потенциалом

10	Разработчики, производители, поставщики программных, технических и программно-технических средств	Внешний нарушитель	со средним потенциалом

Возможная мотивация	Предполагаемые возможности
Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему.
Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему
Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.	Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования

Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, без физического доступа к аппаратным средствам, на которых реализованы СКЗИ и среда их функционирования Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования
Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или злоупотребления доверием	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы

Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны Возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках Возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществлять создание методов и средств реализации атак и реализацию атак на информационную систему Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ) Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)