

**Таблица 1**

	Наименование	эксперт Антон	Эксперт Ратмир	Эксперт Александр
Y1	Угроза жизни или здоровью.	Низкая	Низкая	Высокая
Y1	Унижение достоинства личности.	Средняя	Отсутствует	Средняя
Y1	Нарушение свободы, личной неприкосновенности.	Средняя	Низкая	Высокая
Y1	Нарушение неприкосновенности частной жизни.	Высокая	Высокая	Высокая
Y1	Нарушение личной, семейной тайны, утрата чести и доброго имени.	Средняя	Высокая	Средняя
Y1	Нарушение тайны переписки, телефонных переговоров, иных сообщений.	Высокая	Высокая	Высокая
Y1	<u>Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.</u>	Высокая	Высокая	Высокая
Y1	Финансовый, иной материальный ущерб физическому лицу.	Средняя	Средняя	Высокая
Y1	Нарушение конфиденциальности (утечка) персональных данных.	Высокая	Высокая	Высокая

У1	"Травля" гражданина в сети "Интернет".	Средняя	Низкая	Средняя
----	--	---------	--------	---------

Y1	Разглашение персональных данных граждан	Высокая	Высокая	Высокая
Y2	Нарушение законодательства Российской Федерации.	Высокая	Высокая	Высокая
Y2	Потеря (хищение) денежных средств.	Высокая	Средняя	Высокая
Y2	Недополучение ожидаемой (прогнозируемой) прибыли.	Средняя	Средняя	Средняя
Y2	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.	Средняя	Средняя	Средняя
Y2	Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).	Низкая	Средняя	Средняя

Y2	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.	Средняя	Высокая	Высокая
Y2	Срыв запланированной сделки с партнером.	Низкая	Низкая	Средняя
Y2	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.	Средняя	Средняя	Средняя
Y2	Потеря клиентов, поставщиков.	Средняя	Средняя	Высокая
Y2	Потеря конкурентного преимущества.	Низкая	Средняя	Низкая
Y2	Невозможность заключения договоров, соглашений.	Низкая	Средняя	Высокая
Y2	Нарушение деловой репутации.	Низкая	Низкая	Средняя
Y2	Снижение престижа.	Средняя	Низкая	Средняя
Y2	Дискредитация работников.	Средняя	Низкая	Низкая
Y2	Утрата доверия.	Средняя	Средняя	Низкая
Y2	Причинение имущественного ущерба.	Высокая	Высокая	Высокая
Y2	Неспособность выполнения договорных обязательств.	Средняя	Высокая	Высокая

Y2	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).	Средняя	Средняя	Высокая
Y2	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).	Средняя	Низкая	Низкая
Y2	Принятие неправильных решений.	Средняя	Средняя	Высокая
Y2	Простой информационной системы или сети.		Средняя	Средняя
Y2	Публикация недостоверной информации на веб-ресурсах организации.	Низкая	Низкая	Низкая
Y2	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением.	Средняя	Средняя	Высокая
Y2	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.	Низкая	Низкая	Средняя
Y2	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Высокая	Высокая	Высокая

УЗ	Причинение ущерба жизни и здоровью людей.	Средняя	Средняя	Низкая
УЗ	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения.	Средняя	Низкая	Средняя
УЗ	Прекращение или нарушение функционирования объектов транспортной инфраструктуры.	Отсутствует	Отсутствует	Отсутствует
УЗ	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия).	Отсутствует	Отсутствует	Отсутствует
УЗ	Прекращение или нарушение функционирования сети связи.	Отсутствует	Отсутствует	Отсутствует
УЗ	Отсутствие доступа к государственной услуге.	Отсутствует	Отсутствует	Отсутствует
УЗ	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного	Отсутствует	Отсутствует	Отсутствует

	договора Российской Федерации.			
--	--------------------------------	--	--	--

УЗ	Снижение уровня дохода государственной корпорации, государственной организации или организации с государственным участием.	Отсутствует	Отсутствует	Отсутствует
УЗ	Возникновение ущерба бюджетам Российской Федерации.	Отсутствует	Отсутствует	Отсутствует
УЗ	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка.	Средняя	Высокая	Высокая
УЗ	Вредные воздействия на окружающую среду.	Средняя	Средняя	Низкая
УЗ	Прекращение или нарушение функционирования пункта управления (ситуационного центра).	Средняя	Средняя	Средняя
УЗ	Снижение показателей государственного оборонного заказа.	Отсутствует	Отсутствует	Отсутствует



УЗ	Прекращение или нарушение функционирования информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка.	Отсутствует	Отсутствует	Отсутствует
УЗ	Нарушение законодательства Российской Федерации.	Высокая	Высокая	Высокая
УЗ	Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др.	Средняя	Средняя	Низкая
УЗ	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов.	Средняя	Высокая	Высокая
УЗ	Нарушение общественного правопорядка, возможность потери или снижения уровня контроля за общественным правопорядком.	Отсутствует	Отсутствует	Отсутствует

УЗ	Нарушение выборного процесса.	Отсутствует	Отсутствует	Отсутствует
----	-------------------------------	-------------	-------------	-------------

УЗ	Отсутствие возможности оперативного оповещения населения о чрезвычайной ситуации.	Отсутствует	Отсутствует	Отсутствует
УЗ	Организация пикетов, забастовок, митингов и других акций.	Отсутствует	Средняя	Отсутствует
УЗ	Массовые увольнения.	Средняя	Средняя	Средняя
УЗ	Увеличение количества жалоб в органы государственной власти или органы местного самоуправления.	Средняя	Средняя	Средняя
УЗ	Появление негативных публикаций в общедоступных источниках	Средняя	Средняя	Отсутствует
УЗ	Создание предпосылок к внутривнутриполитическому кризису.	Отсутствует	Отсутствует	Отсутствует
УЗ	Доступ к персональным данным сотрудников органов государственной власти, уполномоченных в области обеспечения обороны, безопасности и правопорядка, высших должностных лиц государственных органов и других лиц государственных органов.	Отсутствует	Отсутствует	Отсутствует
УЗ	Доступ к системам и сетям с целью незаконного использования вычислительных	Средняя	Средняя	Низкая

	мощностей.			
--	------------	--	--	--

УЗ	Использование веб-ресурсов государственных органов для распространения и управления вредоносным программным обеспечением.	Отсутствует	Отсутствует	Отсутствует
УЗ	Утечка информации ограниченного доступа.	Высокая	Средняя	Высокая
УЗ	Непредоставление государственных услуг	Отсутствует	Отсутствует	Отсутствует

Таблица 2

	Наименование	эксперт Антон	Эксперт Ратмир	Эксперт Александр	Оценка
Y1	Угроза жизни или здоровью.	Низкая 2	Низкая 2	Высокая 9	4,3
Y1	Унижение достоинства личности.	Средняя 5	Отсутствует	Средняя 5	3,3
Y1	Нарушение свободы, личной неприкосновенности.	Средняя 5	Низкая 2	Высокая 9	5,3
Y1	Нарушение неприкосновенности частной жизни.	Высокая 9	Высокая 9	Высокая 9	9
Y1	Нарушение личной, семейной тайны, утрата чести и доброго имени.	Средняя 5	Высокая 9	Средняя 5	6,3
Y1	Нарушение тайны переписки, телефонных переговоров, иных сообщений.	Высокая 9	Высокая 9	Высокая 9	9
Y1	<u>Нарушение иных прав и свобод гражданина, закрепленных в Конституции Российской Федерации и федеральных законах.</u>	Высокая 9	Высокая 9	Высокая 9	9
Y1	Финансовый, иной материальный ущерб физическому лицу.	Средняя 5	Средняя 5	Высокая 9	6,3
Y1	Нарушение конфиденциальности (утечка) персональных данных.	Высокая 9	Высокая 9	Высокая 9	9

Y1	"Травля" гражданина в сети "Интернет".	Средняя 5	Низкая 2	Средняя 5	4
Y1	Разглашение персональных данных граждан	Высокая 9	Высокая 9	Высокая 9	9
Y2	Нарушение законодательства Российской Федерации.	Высокая 9	Высокая 9	Высокая 9	9
Y2	Потеря (хищение) денежных средств.	Высокая 9	Средняя 5	Высокая 9	7,6
Y2	Недополучение ожидаемой (прогнозируемой) прибыли.	Средняя 5	Средняя 5	Средняя 5	5
Y2	Необходимость дополнительных (незапланированных) затрат на выплаты штрафов (неустоек) или компенсаций.	Средняя 5	Средняя 5	Средняя 5	5
Y2	Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств).	Низкая 2	Средняя 5	Средняя 5	4

Y2	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса.	Средняя 5	Высокая 9	Высокая 9	7,6
Y2	Срыв запланированной сделки с партнером.	Низкая 2	Низкая 2	Средняя 5	3
Y2	Необходимость дополнительных (незапланированных) затрат на восстановление деятельности.	Средняя 5	Средняя 5	Средняя 5	5
Y2	Потеря клиентов, поставщиков.	Средняя 5	Средняя 5	Высокая 9	7,6
Y2	Потеря конкурентного преимущества.	Низкая 2	Средняя 5	Низкая 2	3
Y2	Невозможность заключения договоров, соглашений.	Низкая 2	Средняя 5	Высокая 9	5,3
Y2	Нарушение деловой репутации.	Низкая 2	Низкая 2	Средняя 5	3
Y2	Снижение престижа.	Средняя 5	Низкая 2	Средняя 5	4
Y2	Дискредитация работников.	Средняя 5	Низкая 2	Низкая 2	3
Y2	Утрата доверия.	Средняя 5	Средняя 5	Низкая 2	4
Y2	Причинение имущественного ущерба.	Высокая 9	Высокая 9	Высокая 9	9

Y2	Неспособность выполнения договорных обязательств.	Средняя 5	Высокая 9	Высокая 9	7,6
----	---	-----------	-----------	-----------	-----



Y2	Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций).	Средняя 5	Средняя 5	Высокая 9	6,3
Y2	Необходимость изменения (перестроения) внутренних процедур для достижения целей, решения задач (реализации функций).	Средняя 5	Низкая 2	Низкая 2	3
Y2	Принятие неправильных решений.	Средняя 5	Средняя 5	Высокая 9	6,3
Y2	Простой информационной системы или сети.		Средняя 5	Средняя 5	3,3
Y2	Публикация недостоверной информации на веб-ресурсах организации.	Низкая 2	Низкая 2	Низкая 2	2
Y2	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением.	Средняя 5	Средняя 5	Высокая 9	6,3
Y2	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и (или) от его имени.	Низкая 2	Низкая 2	Средняя 5	3
Y2	Утечка конфиденциальной информации (коммерческой тайны, секретов производства (ноу-хау) и др.)	Высокая 9	Высокая 9	Высокая 9	9

УЗ	Причинение ущерба жизни и здоровью людей.	Средняя 5	Средняя 5	Низкая 2	4
УЗ	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения.	Средняя 5	Низкая 2	Средняя 5	4

УЗ	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций в системно значимой кредитной организации, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем, системно значимой инфраструктурной организацией финансового рынка.	Средняя 5	Высокая 9	Высокая 9	7,6
УЗ	Вредные воздействия на окружающую среду.	Средняя 5	Средняя 5	Низкая 2	4
УЗ	Прекращение или нарушение функционирования пункта управления (ситуационного центра).	Средняя 5	Средняя 5	Средняя 5	5

УЗ	Нарушение законодательства Российской Федерации.	Высокая 9	Высокая 9	Высокая 9	9
УЗ	Публикация недостоверной социально значимой информации на веб-ресурсах, которая может привести к социальной напряженности, панике среди населения и др.	Средняя 5	Средняя 5	Низкая 2	4
УЗ	Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса, если это ведет к выводу из строя технологических объектов, их компонентов.	Средняя 5	Высокая 9	Высокая 9	7,6

УЗ	Массовые увольнения.	Средняя 5	Средняя 5	Средняя 5	5
УЗ	Увеличение количества жалоб в органы государственной власти или органы местного самоуправления.	Средняя 5	Средняя 5	Средняя 5	5
УЗ	Появление негативных публикаций в общедоступных источниках	Средняя 5	Средняя 5	Отсутствует	3,3
УЗ	Доступ к системам и сетям с целью незаконного использования вычислительных мощностей.	Средняя 5	Средняя 5	Низкая 2	4

Таблица 3

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	
Террористические, экстремистские группировки	-	-	-	-
Преступные группы (криминальные структуры)	-	+ (желание самореализоваться)	-	У2 (невозможность решения задач или снижение эффективности решения задач)
Отдельные физические лица (хакеры)	+ (любопытство или получение финансовой или иной материальной выгоды)	+ (получение финансовой или иной материальной выгоды)	-	У1 (унижение достоинства личности; «травля» гражданина в сети «Интернет»; нарушение конфиденциальности (утечка) персональных данных)

Конкурирующие организации	-	+(получение конкурентных преимуществ)	-	У2 (потеря клиентов, поставщиков) У3 (появление негативных публикаций в общедоступных источниках)
Разработчик и программны х, программно-аппаратных средств	-	+(внедрение дополнительных функциональных возможностей в программные или программно-аппаратные средства на этапе разработки)	-	У2 (невозможность решения задач или снижение эффективности решения задач)
Лица, обеспечивающие поставку программны х, программно-аппаратных средств, обеспечивающих систем	-	+(непреднамеренные, неосторожные или неквалифицированны е действия)	-	У2 (неспособность выполнения договорных обязательств)
Поставщики вычислительных услуг, услуг связи	-	-	-	-

Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	-	+(непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (невозможность решения задач или снижение эффективности решения задач)
Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	-	+(непреднамеренные, неосторожные или неквалифицированные действия)	-	У2 (Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса; необходимость изменения внутренних процедур для достижения целей, решения задач) У3 (доступ к системам и сетям с целью незаконного использования вычислительных мощностей)
Авторизованные пользователи систем и сетей	+(Непреднамеренные, неосторожные или неквалифицированные действия)	+(получение финансовой или иной материальной выгоды)	-	У1 (разглашение персональных данных граждан)

Системные администраторы и администраторы безопасности	-	+(получение финансовой или иной материальной выгоды)	-	У1 нарушение конфиденциальности (утечка) персональных данных У2 (публикация недостоверной информации на веб-ресурсах организации)
Бывшие работники (пользователи)	+(мечь за ранее совершенные действия)	+(мечь за ранее совершенные действия)	-	У1 (нарушение неприкосновенности частной жизни; нарушение тайны переписки, телефонных переговоров, иных сообщений) У2 (снижение престижа; нарушение деловой репутации; утрата доверия)

**Таблица 4**

№ п/п	Виды риска (ущерба) и возможные негативные последствия*	Виды актуального нарушителя**	Категория нарушителя	Уровень возможностей нарушителя
1	У1 унижение достоинства личности; «травля» гражданина в сети «Интернет»; нарушение конфиденциальности (утечка) персональных данных; Разглашение персональных данных граждан; нарушение неприкосновенности частной жизни; нарушение тайны переписки, телефонных переговоров, иных сообщений.	Отдельные физические лица (хакеры)	Внешний	Н3
		Авторизованные пользователи систем и сетей	Внешний	Н1
		Бывшие работники (пользователи)	Внешний	Н1
		Системные администраторы и администраторы безопасности	Внешний Внутренний	Н3
2	У2 невозможность решения задач или	Преступные группы (криминальные структуры)	Внешний	Н2



	<p>снижение эффективности решения задач;</p> <p>потеря клиентов, поставщиков; неспособность выполнения договорных обязательств;</p> <p>Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса;</p> <p>необходимость изменения внутренних процедур для достижения целей, решения задач;</p> <p>публикация недостоверной информации на веб-ресурсах организации;</p> <p>снижение престижа; нарушение деловой</p>	Конкурирующие организации	Внешний	Н1
		Разработчики программных, программно-аппаратных средств	Внешний	Н3
		Лица, обеспечивающие поставку программных, программно-аппаратных средств, обеспечивающих систем	Внешний	Н2
		Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внешний Внутренний	Н4
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие	Внешний Внутренний	Н3

	репутации; утрата доверия	системы оператора (администрация, охрана, уборщики и т.д.)		
		Системные администраторы и администраторы безопасности	Внутренний	Н4
		Бывшие работники (пользователи)	Внешний	Н1
3	УЗ появление негативных публикаций в общедоступных источниках; доступ к системам и сетям с целью незаконного использования вычислительных мощностей	Конкурирующие организации	Внешний	Н1
		Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.)	Внешний Внутренний	Н3

**Таблица 5**

Номер УБИ	Наименование УБИ	Категория нарушителя и его возможности	Какое свойство информации нарушает
УБИ. 001	Угроза автоматического распространения вредоносного кода в грид-системе	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 002	Угроза агрегирования данных, передаваемых в грид-системе	Внешний нарушитель со средним потенциалом	К
УБИ. 004	Угроза аппаратного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом	Ц
УБИ. 005	Угроза внедрения вредоносного кода в BIOS	Внутренний нарушитель с высоким потенциалом	К, Ц, Д

УБИ. 006	Угроза внедрения кода или данных	Внешний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 007	Угроза воздействия на программы с высокими привилегиями	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц
УБИ. 008	Угроза восстановления и/или повторного использования аутентификационной информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К
УБИ. 009	Угроза восстановления предыдущей уязвимой версии BIOS	Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ.012	Угроза деструктивного изменения конфигурации/среды окружения программ	Внутренний нарушитель с	К, Ц, Д

		низким потенциалом	
УБИ. 013	Угроза деструктивного использования декларированного функционала BIOS	Внутренний нарушитель с низким потенциалом	Ц
УБИ. 015	Угроза доступа к защищаемым файлам с использованием обходного пути	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К
УБИ. 018	Угроза загрузки нештатной операционной системы	Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 019	Угроза заражения DNS-кеша	Внешний нарушитель с низким потенциалом	К
УБИ. 022	Угроза избыточного выделения оперативной памяти	Внешний нарушитель с низким потенциалом	Д

		Внутренний нарушитель с низким потенциалом	
УБИ. 023	Угроза изменения компонентов информационной (автоматизированной) системы	Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 024	Угроза изменения режимов работы аппаратных элементов компьютера	Внутренний нарушитель с высоким потенциалом	Ц, Д
УБИ.030	Угроза использования информации идентификации/аутентификации , заданной по умолчанию	Внутренний нарушитель с низким потенциалом  Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ.032	Угроза использования поддельных цифровых подписей BIOS	Внешний нарушитель со средним потенциалом	Ц
УБИ.034	Угроза использования слабостей протоколов сетевого/локального обмена данными	Внешний нарушитель с	К, Ц, Д

		<p>низким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p>	
УБИ.035	Угроза использования слабых криптографических алгоритмов BIOS	Внешний нарушитель с высоким потенциалом	К, Ц, Д
УБИ. 037	Угроза исследования приложения через отчёты об ошибках	<p>Внешний нарушитель со средним потенциалом</p> <p>Внутренний нарушитель со средним потенциалом</p>	К
УБИ.039	Угроза истощения запаса ключей, необходимых для обновления BIOS	Внешний нарушитель со средним потенциалом	Ц
УБИ. 045	Угроза нарушения изоляции среды исполнения BIOS	Внутренний нарушитель с низким потенциалом	К, Ц, Ф

УБИ. 049	Угроза нарушения целостности данных кеша	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ. 051	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания	Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ. 053	Угроза невозможности управления правами пользователей BIOS	Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 059	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Д



УБИ. 063	Угроза некорректного использования функционала программного и аппаратного обеспечения	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 067	Угроза неправомерного ознакомления с защищаемой информацией	Внутренний нарушитель с низким потенциалом	К
УБИ. 068	Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 071	Угроза несанкционированного восстановления удалённой защищаемой информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с	К

		низким потенциалом	
УБИ. 072	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS	Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 074	Угроза несанкционированного доступа к аутентификационной информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К
УБИ. 083	Угроза несанкционированного доступа к системе по беспроводным каналам	Внешний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 084	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д

УБИ. 086	Угроза несанкционированного изменения аутентификационной информации	<p>Внешний нарушитель с низким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p>	Ц, Д
УБИ. 087	Угроза несанкционированного использования привилегированных функций BIOS	<p>Внешний нарушитель с высоким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p>	К, Ц, Д
УБИ. 088	Угроза несанкционированного копирования защищаемой информации	<p>Внешний нарушитель с низким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p>	К .

УБИ. 089	Угроза несанкционированного редактирования реестра	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 090	Угроза несанкционированного создания учётной записи пользователя	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 091	Угроза несанкционированного удаления защищаемой информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Д

УБИ. 093	Угроза несанкционированного управления буфером	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 094	Угроза несанкционированного управления синхронизацией и состоянием	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	Ц, Д
УБИ. 095	Угроза несанкционированного управления указателями	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со	К, Ц, Д

		средним потенциалом	
УБИ. 099	Угроза обнаружения хостов	Внешний нарушитель с низким потенциалом	К
УБИ. 100	Угроза обхода некорректно настроенных механизмов аутентификации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 102	Угроза опосредованного управления группой программ через совместно используемые данные	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	Ц, Д
УБИ. 103	Угроза определения типов объектов защиты	Внешний нарушитель с	К

		низким потенциалом	
УБИ. 107	Угроза отключения контрольных датчиков	Внешний нарушитель с высоким потенциалом  Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ. 109	Угроза перебора всех настроек и параметров приложения	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	Ц, Д
УБИ. 110	Угроза перегрузки грид-системы вычислительными заданиями	Внутренний нарушитель с низким потенциалом	Д
УБИ. 111	Угроза передачи данных по скрытым каналам	Внешний нарушитель со	К

		<p>средним потенциалом</p> <p>Внутренний нарушитель со средним потенциалом</p>	
УБИ. 112	Угроза передачи запрещённых команд на оборудование с числовым программным управлением	Внутренний нарушитель с низким потенциалом	Ц
УБИ. 113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	<p>Внешний нарушитель с низким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p>	Ц, Д
УБИ. 114	Угроза переполнения целочисленных переменных	<p>Внешний нарушитель со средним потенциалом</p> <p>Внутренний нарушитель со</p>	К, Ц, Д



		средним потенциалом	
УБИ. 115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К
УБИ. 116	Угроза перехвата данных, передаваемых по вычислительной сети	Внешний нарушитель с низким потенциалом	К
УБИ. 117	Угроза перехвата привилегированного потока	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д

УБИ. 118	Угроза перехвата привилегированного процесса	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 121	Угроза повреждения системного реестра	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ. 122	Угроза повышения привилегий	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д

УБИ. 123	Угроза подбора пароля BIOS	Внутренний нарушитель с низким потенциалом	К, Д
УБИ. 124	Угроза подделки записей журнала регистрации событий	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Ц
УБИ. 127	Угроза подмены действия пользователя путём обмана	Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 128	Угроза подмены доверенного пользователя	Внешний нарушитель с низким потенциалом	К
УБИ. 129	Угроза подмены резервной копии программного обеспечения BIOS	Внутренний нарушитель с низким потенциалом	Ц

УБИ. 132	Угроза получения предварительной информации об объекте защиты	Внешний нарушитель со средним потенциалом	К
УБИ. 139	Угроза преодоления физической защиты	Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 140	Угроза приведения системы в состояние «отказ в обслуживании»	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Д
УБИ. 144	Угроза программного сброса пароля BIOS	Внутренний нарушитель с низким потенциалом	К, Ц
УБИ. 145	Угроза пропуска проверки целостности программного обеспечения	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с	Ц, Д

		низким потенциалом	
УБИ. 149	Угроза сбоя обработки специальным образом изменённых файлов	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 150	Угроза сбоя процесса обновления BIOS	Внутренний нарушитель со средним потенциалом	Д
УБИ. 152	Угроза удаления аутентификационной информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д

УБИ. 154	Угроза установки уязвимых версий обновления программного обеспечения BIOS	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 155	Угроза утраты вычислительных ресурсов	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Д
УБИ. 156	Угроза утраты носителей информации	Внутренний нарушитель с низким потенциалом	К, Д
УБИ. 157	Угроза физического вывода из строя средств хранения, обработки и (или)	Внешний нарушитель с низким потенциалом	Ц, Д

	ввода/вывода/передачи информации		
УБИ. 158	Угроза форматирования носителей информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ. 160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации	Внешний нарушитель с низким потенциалом	К, Д
УБИ. 162	Угроза эксплуатации цифровой подписи программного кода	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д

УБИ. 165	Угроза включения в проект не достоверно испытанных компонентов	Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 170	Угроза неправомерного шифрования информации	Внешний нарушитель с низким потенциалом	Д
УБИ. 176	Угроза нарушения технологического/производственного процесса из-за временных задержек, вносимых средством защиты	Внешний нарушитель с низким потенциалом	Д
УБИ. 177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью	Внутренний нарушитель с низким потенциалом	Ц, Д
УБИ. 182	Угроза физического устаревания аппаратных компонентов	Внутренний нарушитель с низким потенциалом	Д
УБИ. 183	Угроза перехвата управления автоматизированной системой управления технологическими процессами	Внешний нарушитель с высоким потенциалом	Ц, Д



		Внутренний нарушитель со средним потенциалом	
УБИ. 185	Угроза несанкционированного изменения параметров настройки средств защиты информации	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 187	Угроза несанкционированного воздействия на средство защиты информации	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 188	Угроза подмены программного обеспечения	Внутренний нарушитель со	К, Ц, Д

		средним потенциалом	
УБИ. 189	Угроза маскирования действий вредоносного кода	Внешний нарушитель со средним потенциалом	Ц, Д
УБИ. 190	Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет	Внешний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 192	Угроза использования уязвимых версий программного обеспечения	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д

УБИ. 198	Угроза скрытной регистрации вредоносной программой учетных записей администраторов	Внешний нарушитель со средним потенциалом	Ц
УБИ. 203	Угроза утечки информации с неподключенных к сети Интернет компьютеров	Внешний нарушитель со средним потенциалом  Внутренний нарушитель со средним потенциалом	К
УБИ. 204	Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров	Внешний нарушитель со средним потенциалом	Ц
УБИ. 205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты	Внешний нарушитель с низким потенциалом	Д
УБИ. 207	Угроза несанкционированного доступа к параметрам настройки	Внешний нарушитель с	К, Ц, Д

	оборудования за счет использования «мастер-кодов» (инженерных паролей)	<p>низким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p>	
УБИ. 208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники	<p>Внешний нарушитель с низким потенциалом</p> <p>Внутренний нарушитель с низким потенциалом</p> <p>Внешний нарушитель со средним потенциалом</p> <p>Внутренний нарушитель со средним потенциалом</p>	Д

УБИ. 209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора	Внешний нарушитель с низким потенциалом  Внутренний нарушитель с низким потенциалом	К, Ц, Д
УБИ. 210	Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения	Внутренний нарушитель с высоким потенциалом	Ц,Д
УБИ.			
УБИ. 212	Угроза перехвата управления информационной системой	Внутренний нарушитель со средним потенциалом	К, Ц, Д
УБИ. 213	Угроза обхода многофакторной аутентификации	Внешний нарушитель с высоким потенциалом	К, Ц, Д
УБИ. 214	Угроза несвоевременного выявления и реагирования компонентами информационной (автоматизированной) системы	Внутренний нарушитель со	Ц, Д

	(в том числе средствами защиты информации) на события безопасности информации	средним потенциалом	
УБИ. 217	Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения	Внутренний нарушитель со средним потенциалом  Внешний нарушитель со средним потенциалом	К, Ц, Д