

Риски в системе безопасности информационных систем школы

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
Технологические риски					
Доступ к данным посторонних	10%	Регулярный инструктаж по информационной безопасности. Замена паролей, например, генерирование. Конфиденциальность.	Запись паролей в доступных для посторонних местах, доверительная передача данных стороннему лицу.	Нарушение федерального законодательства (доступность персональных данных). Хищение данных служебного пользования	Регулярный инструктаж по информационной безопасности. Наложение личной ответственности локальным актом школы, определить уровни допуска к данным для пользователей. Регулярная смена паролей, использование сложных паролей.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
Взлом паролей пользователей	3 %	<p>Установка комплексной системы защиты компьютерной сети, которую обеспечат специализированные программы, выявляющие все возможные угрозы безопасности и применяющие меры по борьбе с ними.</p> <p>Использование дополнительных программ, которые блокируют подключение неизвестных устройств.</p> <p>Разработка регламента работы с информационными ресурсами.</p>	<p>Поиск пароля по хешу.</p> <p>Кража Cookie.</p> <p>Фишинговые атаки (включают в себя использование специально созданного электронного письма, чтобы заманить получателя на слив его личной или финансовой информации).</p> <p>Кейлоггинг (позволяет хакерам и злоумышленникам записывать нажатия клавиш, которые вы совершаете).</p> <p>Атаки Brute Force (подбор пароля с использованием специальных программ).</p> <p>Атаки по словарю.</p>	<p>Доступ к данным.</p> <p>Изменение данных.</p> <p>Копирование данных.</p> <p>Потеря репутации.</p>	<p>Разъяснительная работа среди сотрудников и учащихся по информационной безопасности.</p> <p>Использование сложных паролей.</p> <p>Частая смена паролей.</p> <p>Лучший метод предотвратить кражу Cookie - избегать общедоступных и незащищенных частных сетей, использовать VPN для шифрования и туннелировать соединение на мобильном телефоне, не забывать чистить куки.</p> <p>Нужно сохранять бдительность и руководствоваться здравым смыслом. Если вы не уверены в электронном письме</p>

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
					или сообщении, спросите человека, который предположительно отправил его, чтобы убедиться, что сообщение безопасно открыть.
Подсматривание пароля у пользователей	50 %	Ограничение доступа посторонних лиц в помещение. Использование сложных паролей. Частая смена		Доступ к данным. Изменение данных. Копирование данных. Потеря репутации.	Ограничение доступа посторонних лиц в помещение. Использование сложных паролей.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
		паролей.			Частая смена паролей.
Выманивание пароля у пользователей (обман, психологические манипуляции)	5 %	Разъяснительная профилактическая работа по информационной безопасности.	Доверительные отношения. Отвлечение внимания.	Доступ к данным. Изменение данных. Копирование данных. Потеря репутации.	Обучение основам информационной безопасности, разъяснительная работа.
Выявление паролей снифером (перехват сетевых пакетов)	1%	Наличие грамотного специалиста в штате, способного обнаружить и предотвратить стороннее вмешательство в программное обеспечение.	Подмена IP-адреса. Внедрение программ, позволяющих прослушивание сети с помощью программ сетевых анализаторов	Перехват данных позволяет получить передаваемые по сети пароли, конфиденциальные письма и др.	В школе такого специалиста нет.
Разрушение носителей данных (жестких дисков, систем хранения)	10%	Соблюдение правил эксплуатации при работе с носителем. Резервное копирование данных.	Запуск вредоносной программы или вируса. Преднамеренное вредительство (физическое нарушение целостности носителя). Непреднамеренное физическое повреждение жесткого диска, вызванное	Потеря данных. Сбой в работе системы	Определение спектра лиц, отвечающих за резервное копирование данных по профилю своей деятельности.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
			падением или неаккуратным обращением		
Разрушение данных из-за сбоя питания	10%	<p>Использование источников бесперебойного питания.</p> <p>Соблюдение правил эксплуатации при работе с носителем.</p> <p>Резервное копирование данных.</p>	<p>Обесточивание.</p> <p>Скачок напряжения, вызванный либо по вине компании, подающей электроэнергию, либо по причине сторонних причин.</p>	<p>Потеря данных.</p> <p>Сбой в работе системы</p>	<p>Покупка источников бесперебойного питания.</p> <p>Определение спектра лиц, отвечающих за резервное копирование данных по профилю своей деятельности.</p>
Разрушение данных из-за перегрева носителя	5%	<p>Использование источников бесперебойного питания.</p> <p>Соблюдение правил эксплуатации оборудования.</p> <p>Резервное копирование данных.</p>	Неправильное использование оборудования (преднамеренное или непреднамеренное).	<p>Неисправимые повреждения поверхности винчестера, поломка системы магнитных головок, которые могут «вспороть» винчестер и уничтожить хранящуюся на нём информацию.</p> <p>Помимо потери данных, тепло может</p>	<p>Разъяснение правил эксплуатации оборудования.</p> <p>Резервное копирование данных.</p>

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
				<p>вывести из строя материнскую плату, процессор и другие комплектующие.</p> <p>Возможно замедление скорости работы компьютера и его самостоятельного выключения или циклической перезагрузки.</p> <p>Потеря данных без возможности восстановления.</p>	
Утрата / порча данных по неосторожности	50%	При установке нового программного обеспечения воспользоваться помощью специалиста.	Случайное форматирование жесткого диска. Забывчивость при завершении работы.	Потеря данных без возможности восстановления.	<p>Правильная эксплуатация оборудования (правильно выключать компьютер, выходить из всех активных программ корректно).</p> <p>Повышение информационной грамотности.</p>

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
					Выполнение диагностики оборудования специалистами (не самостоятельно!)
Утечка персональных данных	5 %	<p>Соблюдение федерального законодательства в области сохранения персональных данных.</p> <p>Использование антивирусных и криптографических программ.</p> <p>Копирование значимой информации на внешние жесткие диски.</p> <p>Установление паролей и их регулярная замена.</p>	Незнание законодательства, халатность сотрудников, хакерские атаки.	Мошенничество, передача третьим лицам.	<p>Составлен локальный акт, регламентирующий сохранение и обработку персональных данных.</p> <p>Получены письменные заявления-согласия родителей об использовании отдельных персональных данных детей.</p> <p>Использование антивирусных и криптографических программ.</p> <p>Копирование значимой информации на внешние жесткие диски.</p>
Утечка иных	5%	Соблюдение	Невнимательное	Мошенничество,	Установка КриптоПро.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
конфиденциальных данных		<p>федерального законодательства в области сохранения персональных данных.</p> <p>Использование антивирусных и криптографических программ.</p> <p>Копирование значимой информации на внешние жесткие диски.</p> <p>Установление паролей и их регулярная замена.</p>	<p>обращение сотрудников с информацией.</p> <p>Халатность сотрудников.</p> <p>Хакерские атаки.</p>	<p>передача третьим лицам.</p> <p>Незаконное тиражирование, копирование.</p>	<p>Обучение основам информационной безопасности, разъяснительная работа.</p>
Массовое заражение компьютерным вирусом	10%	<p>Установка антивирусных программ.</p> <p>Соблюдение правил «компьютерной гигиены».</p>	<p>Окончание сроков лицензий ПО.</p> <p>Пиратское программное обеспечение.</p> <p>Использования зараженных вирусом</p>	<p>Заражение компьютерным вирусом.</p> <p>Потеря данных.</p> <p>Сбой в работе системы.</p>	<p>Своевременное обновление антивирусных программ.</p> <p>Обучение основам информационной безопасности,</p>

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
			<p>носителей (флеш-карты, переносные жесткие диски и др.).</p> <p>Прочтение зараженного файла, прикрепленного к электронному письму.</p> <p>Коллективное пользования зараженными файлами в сети.</p> <p>Посещение вебсайтов, использующих бреши в безопасности системы для уничтожения информации.</p>		<p>«компьютерной гигиены».</p> <p>Регулярный мониторинг программного обеспечения, правильного использования оборудования.</p>
Сбои в работе Интернет во время занятий	30%	<p>Обеспечение работоспособности компьютерного парка (заключение договора сна обслуживание технических средств).</p> <p>Подключение высокоскоростного интернета.</p>	<p>Плохой сигнал беспроводной сети.</p> <p>Плохое подключение к интернету.</p> <p>Неправильная работа модема.</p>	Нарушение плана занятий.	Подключение высокоскоростного интернета.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
			Неисправность порта подключения.		
Несанкционированное подключение к системе видеонаблюдения (если есть)	5%	Соблюдение инструкций охранной службой.	Отвлечение охранника.	Сбой работы системы видеонаблюдения	Подключение к системе возможно только ответственными лицами. В точке доступа всегда находится охранник.
Репутационные риски					
В связи с неудачной (некорректной) публикацией	5%	Контроль над качеством транслируемой информации.	Несогласованные публикации. Безответственность сотрудников.	Урон деловой репутации школы.	Создание внутренних регламентов по информационной политике.
Некорректное ведение дискуссий в соцсети	25%	Корпоративная культура.	Множество вариантов, полная непредсказуемость.	Формирование отрицательного имиджа сотрудников, как следствие – урон имиджу школы.	Профилактические беседы в целях формирования информационной культуры.
Жесткая критика школы в сети	10%	Своевременная разъяснительная работа с педагогическим коллективом, с учащимися, родителями.	Множество вариантов, которые можно пропустить при мониторинге соцсетей.	Создание отрицательного имиджа школы. Формирование негативного общественного мнения.	Формирование положительного имиджа школы в СМИ, соцсетях, на массовых мероприятиях, родительских собраниях и др.. Мониторинг соцсетей.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
Публикации на сайте с нарушением авторских прав	5%	Контроль над качеством публикуемой информации.	Личная безответственность сотрудников.	Урон деловой репутации, судебные разбирательства, финансовые потери.	Информирование об авторских правах и ответственности. Воспитание информационной культуры.
Появление некорректных (не актуальных, не проверенных) данных на сайте	5%	Контроль над качеством публикуемой информации.	Недостаточное внимание сотрудников.	Урон деловой репутации.	Контроль над качеством и достоверностью публикуемой информации.
Кибербуллинг учеников	10%	Профилактические беседы по правилам поведения в социальных сетях. Ежедневный мониторинг социальных сетей классными руководителями.	Анонимные аккаунты, взлом личных страниц	Рост негатива к данным ученикам со стороны социума, подавленное психологическое состояние учеников.	Профилактические беседы по правилам поведения в социальных сетях. Ежедневный мониторинг социальных сетей классными руководителями. Психолого-педагогическая помощь пострадавшим от насилия, предупреждение суицидальных попыток.

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
Кибербуллинг учителей	5%	<p>Профилактические беседы по правилам поведения в социальных сетях.</p> <p>Введение правил использования мобильных телефонов и других гаджетов в школе.</p>	Нарушение правил использования гаджетов в школе. Проявление агрессии.	<p>Формирование отрицательного имиджа школы, учителя.</p> <p>Нервное напряжение учителя, ухудшение психологического климата на уроках, понижение качества работы.</p>	<p>Разработка локальных актов по правилам пользования телефонами, планшетами и др. электронными устройствами в школе.</p> <p>Психологическая поддержка учителя в случае кибербуллинга.</p>
Кибербуллинг администрации	5%	<p>Профилактические беседы по правилам поведения в социальных сетях.</p> <p>Введение правил использования мобильных телефонов и других гаджетов в школе.</p>	Нарушение правил использования гаджетов в школе. Проявление агрессии.	<p>Формирование отрицательного имиджа школы, учителя.</p> <p>Нервное напряжение учителя, ухудшение психологического климата на уроках, понижение качества работы.</p>	<p>Разработка локальных актов по правилам пользования телефонами, планшетами и др. электронными устройствами в школе.</p> <p>Психологическая поддержка учителя в случае кибербуллинга.</p>
Политическая агитация или иная нежелательная или запрещенная	5%	<p>Информационная политика школы.</p> <p>Создание перечня</p>	<p>Хакерские атаки.</p> <p>Вредоносные программы.</p>	Привлечение к административной ответственности.	<p>Установка контент-фильтров.</p> <p>Мониторинг и</p>

Риск	Вероятность наступления (%)	Возможные меры защиты (предотвращения или минимизации)	Варианты обхода защиты	Последствия в случае наступления	Ваши действия именно в вашей школе
информация на сайте или в информационных системах		<p>источников, которые могут травмировать психику детей.</p> <p>Разработка порядка доступа детей к сети Интернет в школе.</p> <p>Частичный запрет на пользование собственными носителями информации.</p> <p>Установка контент-фильтры на школьные компьютеры.</p>	<p>Нежелательный рекламный контент.</p> <p>Окончание сроков работы антивирусных программ.</p> <p>Отключение контент-фильтров.</p>	Отрицательное воздействие на репутацию, имидж учреждения.	<p>обновление антивирусных программ.</p> <p>Информационное просвещение родителей по информационной безопасности.</p>
Другие риски					
Неправомерное требование предоставления персональных данных различными организациями.	10%	Выстраиванию правильных внутренних и внешних коммуникаций.	Психологическое давление на сотрудников.	Отрицательное воздействие на репутацию, имидж учреждения.	Защита информации (отказ выполнения устных и/или неправомерных запросов).