Автор: Шумков К.В., Тазетдинова Ю.А., Тазетдинов Б.И.
14.11.2025 10:06 - Обновлено 28.11.2025 11:01

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАНИИ: МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ВРЕДОНОСНЫМ ПРОГРАММАМ

Шумков К.В., студент 1 курса БФ

Тазетдинова Ю.А., к.ф.-м.н., доцент

Тазетдинов Б.И., к.ф.-м.н., доцент

г. Бирск, Бирский филиал Уфимского университета науки и технологий

Аннотация. Работа посвящена актуальной проблеме обеспечения цифровой безопасности в современной образовательной среде. Рассматриваются основные виды угроз, связанные с вредоносным программным обеспечением (ПО), и их потенциальное воздействие на учебный процесс, конфиденциальность данных и функциональность образовательных учреждений. В работе проанализированы ключевые уязвимости образовательных систем и предложен комплекс организационных и технических методов противодействия киберугрозам. Особое внимание уделяется роли формирования цифровой грамотности и культуры кибербезопасности среди всех участников образовательного процесса: учащихся, педагогов и администрации. Статья предназначена для руководителей образовательных организаций, учителей информатики и всех специалистов, занимающихся внедрением и поддержкой цифровой

инфраструктуры в сфере образования.

Ключевые слова: цифровая безопасность, вредоносное ПО, киберугрозы, фишинг, цифровая грамотность, информационная гигиена, защита данных.

Введение. Современное образование немыслимо без использования цифровых технологий: от электронных дневников и образовательных платформ до облачных сервисов и онлайн-библиотек. Однако интенсивная цифровизация делает образовательные учреждения лакомой мишенью для киберпреступников. Школы, колледжи и университеты зачастую обладают ценными данными (персональные данные учащихся и сотрудников, научные исследования), но при этом не имеют достаточных ресурсов для выстраивания полноценной системы защиты.

Вредоносное ПО представляет собой одну из наиболее распространенных и опасных угроз. Оно может привести к парализации учебного процесса, утечке конфиденциальной информации, финансовым потерям и репутационному ущербу для учреждения. В данной статье систематизируются основные виды вредоносных программ, актуальные для образовательной сферы, и предлагаются практические методы построения многоуровневой системы защиты, сочетающей технические решения и воспитание осознанного поведения пользователей.

1. Угрозы и уязвимости образовательной среды. Образовательные учреждения характеризуются рядом специфических уязвимостей, которые делают их привлекательной мишенью для киберпреступников. Ключевой проблемой является

высокая мобильность пользователей: массовое использование личных устройств учащихся и преподавателей по модели BYOD (Bring Your Own Device) значительно расширяет периметр защиты, усложняя контроль за безопасностью. Эта ситуация усугубляется выраженной разнородностью IT-инфраструктуры, где одновременная эксплуатация устаревшего и современного оборудования и программного обеспечения создает многочисленные бреши в безопасности, которыми может воспользоваться злоумышленник. Серьёзным ограничением выступает хроническая ограниченность ресурсов, выражающаяся в недостаточном финансировании IT-безопасности и острой нехватке квалифицированных кадров. Наконец, фундаментальной уязвимостью остается низкий уровень цифровой грамотности, из-за чего учащиеся и часть педагогического состава зачастую не способны распознать классические методы социальной инженерии.

Среди основных типов вредоносного ПО, представляющих непосредственную угрозу для учебного процесса, наиболее опасными являются программы-вымогатели (Ransomware), которые шифруют данные на серверах и рабочих станциях, требуя выкуп за их восстановление, что может полностью парализовать деятельность учреждения. Не менее распространена угроза фишинга, когда рассылаются письма и сообщения, маскирующиеся под официальные уведомления от администрации или популярных сервисов, с целью похищения учетных данных. Скрытную, но постоянную опасность представляет шпионское ПО (Spyware), которое тайно собирает информацию о действиях пользователя, перехватывая пароли и личные данные. Кроме того, значительный риск связан с созданием ботнетов, когда зараженные компьютеры учебного заведения могут быть использованы злоумышленниками для проведения масштабных скоординированных кибератак.

2. Комплекс методов противодействия. Борьба с вредоносным ПО требует комплексного подхода, включающего технические, организационные и образовательные меры. В основе технической защиты лежит установка и регулярное обновление антивирусного ПО на всех устройствах – от серверов до мобильных гаджетов, что создает базовый уровень безопасности. Не менее важно применение межсетевых экранов для фильтрации сетевого трафика, своевременное обновление

операционных систем и прикладного программного обеспечения для устранения известных уязвимостей, а также использование систем фильтрации контента для блокировки доступа к потенциально опасным веб-ресурсам. Ключевыми элементами инфраструктурной защиты являются сегментация сети, которая ограничивает распространение угроз путем разделения на изолированные сегменты для разных групп пользователей, и регулярное создание резервных копий критически важных данных по правилу 3-2-1, обеспечивающее восстановление работоспособности после возможных инцидентов.

Организационные меры предполагают разработку и внедрение четкой политики информационной безопасности, регламентирование процедур использования личных устройств в учебной сети, проведение регулярных аудитов ИТ-инфраструктуры и создание плана реагирования на инциденты для минимизации ущерба в случае успешной атаки. Однако наиболее значимым для долгосрочной эффективности является образовательный компонент, направленный на формирование культуры кибербезопасности. Это включает проведение регулярных обучающих семинаров и уроков цифровой грамотности для учащихся всех возрастов, специализированные инструктажи для педагогов и администрации по распознаванию фишинговых писей и безопасной работе с данными, использование интерактивных форматов в виде квестов и деловых игр для отработки навыков на практике, а также постоянное информирование о правилах создания надежных паролей и использования двухфакторной аутентификации. Только сочетание этих трех компонентов создает устойчивую систему противодействия современным киберугрозам в образовательной среде.

3. Как защититься от вредоносного ПО. Для построения надежной защиты от киберугроз необходим комплексный подход, включающий три ключевых уровня. Первый уровень – техническая защита. Начните с установки и правильной настройки специального программного обеспечения, которое формирует ваш базовый защитный периметр. Основой защиты является антивирусное ПО от проверенного производителя, которое обнаруживает и блокирует вредоносные программы. Крайне важно не устанавливать одновременно несколько антивирусов, так как они будут конфликтовать

друг с другом. Обязательно активируйте проактивную защиту, включающую эвристический и поведенческий анализ, для выявления ранее неизвестных угроз. Дополните защиту брандмауэром, контролирующим сетевой трафик и блокирующим подозрительные соединения. При работе в интернете используйте современные браузеры со встроенной защитой от фишинга и установите блокировщик рекламы, который также предотвращает доступ к вредоносным рекламным сетям. Будьте предельно внимательны при установке расширений – используйте только официальные магазины и тщательно проверяйте отзывы.

Второй и самый важный уровень – поведенческая защита, или соблюдение "кибергигиены". Никакой антивирус не способен полностью компенсировать невнимательность пользователя. Проявляйте особую осторожность при работе с электронной почтой и сообщениями: не открывайте подозрительные вложения, проверяйте адреса отправителей и помните, что легальные организации никогда не запрашивают конфиденциальные данные через эти каналы. Загружайте программы исключительно с официальных сайтов разработчиков и внимательно читайте каждый шаг установки, чтобы избежать инсталляции нежелательного дополнительного ПО. Обязательно используйте уникальные сложные пароли для каждого важного сервиса и активируйте двухфакторную аутентификацию, которая становится главным щитом даже в случае компрометации пароля. В публичных сетях Wi-Fi используйте VPN для передачи важных данных и избегайте использования непроверенных USB-носителей.

Третий уровень – административная защита, обеспечивающая актуальность и целостность системы. Регулярно обновляйте все компоненты: операционную систему с включенными автоматическими обновлениями, браузеры и приложения, особенно те, что содержат критически важные плагины. Резервное копирование важных данных на внешние носители или в облачные хранилища с историей версий является вашим последним рубежом обороны против программ-вымогателей. Наконец, для повседневных задач работайте под учетной записью с ограниченными правами – это предотвратит большинство попыток вредоносных программ критически изменить систему. Только сочетание этих трех уровней защиты создает действительно устойчивую систему безопасности.

4. Что делать, если вы подозреваете заражение. При обнаружении заражения вредоносным программным обеспечением необходимо немедленно предпринять следующие действия. В первую очередь требуется физически отключиться от интернета – выдернуть сетевой кабель или отключить Wi- Fi соединение. Это критически важное действие прерывает канал связи вредоноса с злоумышленником, блокируя возможность кражи данных и получения вирусом дополнительных команд. После изоляции устройства от сети следует немедленно запустить полную антивирусную проверку системы с использованием установленного защитного решения. Однако следует учитывать, что стандартный антивирус может оказаться неэффективным против сложных угроз, поэтому следующий этап включает использование специальных утилит-сканнеров, таких как Malwarebytes AdwCleaner, Dr.Web CureIt! или Kaspersky Virus Removal Tool. Эти специализированные инструменты способны обнаруживать и нейтрализовать вредоносные программы, которые остались незамеченными основным антивирусным ПО.

В ситуации, когда самостоятельные меры не приносят результата, необходимо обратиться за помощью на специализированные форумы, такие как VirusInfo, где эксперты могут предоставить индивидуальные рекомендации по очистке системы, или же воспользоваться услугами профессиональных IT-специалистов. Особый протокол действий требуется при атаке программ-шифровальщиков (ransomware): категорически не рекомендуется выплачивать требования злоумышленников, поскольку вероятность восстановления файлов после оплаты выкупа минимальна, а такие действия лишь финансируют преступную деятельность. Вместо этого следует обратиться в правоохранительные органы и проверить на сайтах антивирусных компаний наличие бесплатных дешифраторов, которые могли быть разработаны для конкретной версии вируса-шифровальщика.

Заключение. Цифровая безопасность образовательного учреждения – это не просто техническая задача, а комплексная стратегическая цель. Успешное противодействие вредоносному ПО требует симбиоза технологических решений, четких организационных

процедур и, что наиболее важно, непрерывного образования всех участников процесса.

Инвестиции в создание культуры кибербезопасности окупаются многократно, снижая человеческий фактор – основное слабое звено в любой системе защиты. Только сочетая «железо», программное обеспечение и «мягкие» навыки пользователей, можно создать устойчивую образовательную среду, в которой технологии служат развитию, а не становятся источником кризиса. Будущее цифровой безопасности в образовании лежит в области проактивной защиты, где предупреждение угроз становится неотъемлемой частью повседневной цифровой гигиены.

Литература

1. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

2. Приказ Минцифры России от 29.12.2022 № 1292 «Об утверждении Требований к обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

3. Сайт Энциклопедия «Касперского». – URL: https://encyclopedia.kaspersky.ru/knowledge/malware-protection-methods-and-techniques/
(дата обращения: 10.11.2025).

4. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. – Екатеринбург: Изд-во Урал. ун-та, 2019. – 204 с.