## *Секция «Актуальные проблемы информационной безопасности», научный руководитель – Ищукова Е.А., канд. техн. наук, доцент*

### МУЛЬТИФАКТОРНАЯ АУТЕНТИФИКАЦИЯ КАК ФАКТОР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ АТТЕСТАЦИИ СТУДЕНТОВ

Инджиев А.Н., Горяев В.М.

*Калмыцкий государственный университет, Элиста, e-mail: goryaeff@rambler.ru*

В ходе своих исследований на кафедре ИТ мы разрабатываем программно- аппаратный комплекс, который позволяет достоверно идентифицировать студента. В современных условиях средние и высшие учебные заведения хотят продвинуть качество услуг для своих сотрудников и студентов в цифровом образовательном пространстве. В последнее время мы наблюдаем увеличение интенсивности использования новых интернет- приложений в учбеных заведениях, что ведет к многочисленным сопутствующим проблемами.

Безопасный доступ к приложениям электронного обучения и внутренним сетям крайне важен, из-за конфиденциального характера данных. Цифровые данные администрации, сотрудников и студентов должны быть защищены. Именно поэтому все больше вузов признает важность продвинутых решений при идентификации. Специалисты по безопасности давно рекомендуют менять опасные статические пароли на более безопасные динамично произведенные одноразовые пароли. Они могут только использоваться однажды, таким образом устраняя несанкционированный доступ к конфиденциальным данным.

Проблемы, которые могут возникнуть при плохом уровне безопасности:

1. Кража персональных данных
2. Несанкционированный доступ к данным
3. Мошенничество в онлайн
4. Фишинг – вид интернет-мошенничеств и т.д.

Данная работа посвящена «сильным» решениям для идентификации в образовательном процессе для колледжей, университетов, школ. Сильная идентификация предлагает продвинутую безопасность для сотрудников, преподавателей, продавцов и студентов.

Данная работа была направлена на обеспечения «сильной» верификации в процессе различных аттестаций студентов и курсантов. Для ускорения процесса авторизации можно воспользоваться специальным сформированный одноразовым QR-кодом, соотнесенным с конкретной группой или преподавателем и распознанным перед видеокамерой терминала. QR-код можно получить при выборе группы, он отображается на экране и его можно сфотографировать на смартфон, также его можно будет получить с любого компьютера внутренней сети университета (через логин и пароль) и распечатать на принтере.

Компьютер преподавателя должен быть оснащен web-камерой и функцией распознавания лиц. На компьютере формируется QR-код для экзамена. Студент, вызванный на экзамен подходит с этим графическим кодом к считывающему устройству (смартфон или компьютер), затем QR-код отсылает на определенную страницу университетского сайта, где идет распознавание экзаменуемого и в случае успешной завершения процесса выдается квиток с билетом (в противном случае придется выполнять документоориентированное опознавание лица). В общем случае, обладая уникальным QR-кодом можно получить доступ к режиму обучения распознаванию лиц для более лучшей идентификации.

Наиболее интересно использовать мультифакторную аутентификацию для студентов заочной формы обучения и, особенно, для обучаемых в рамках дистанционного обучения, когда нет уверенности в том, что экзамен сдает зарегистрированный в вузе учащийся, а не проплаченный двойник. Для дистанционного обучения используется тот же алгоритм: студент во время сессии заходит в свой личный кабинет и получает сгенерированный QR-код, затем продемонстрировав камере этот код ожидает распознавания личности несколько секунд для доступа к экзамену. Время от времени компьютер сверяется с базой открытой QR-кодом для того, чтобы можно было достоверно выявить зловредные манипуляции в процессе экзамена.

### МОНИТОРИНГ СОБЫТИЙ И ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ SIEM-СИСТЕМ

Канев А.Н.

*Университет ИТМО, Санкт-Петербург, e-mail: ta1ler93@mail.ru*

Обеспечение информационной безопасности (ИБ) является важной задачей для различных организаций. Выполнение этой нетривиальной задачи требует значительных финансовых и трудовых затрат. Важно понимать, что эти затраты сделаны впустую, если система защиты информации при этом действует недостаточно быстро и продуктивно. Поэтому в последнее время все актуальнее становится проблема мониторинга событий ИБ (далее – событий), а также обнаружение и обработка возникающих инцидентов ИБ (далее – инцидентов) в минимальные сроки.

Ключевым понятием в рассматриваемой области является «событие информационной безопасности», для которого в современном законодательстве принято следующее определение:

Событие – идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики ИБ или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности [1, 2].

Мониторинг событий производится на основе данных, полученных из различных источников, к которым относятся:

- IDS/IPS-системы;
- средства антивирусной защиты;
- журналы событий;
- сканеры уязвимостей;
- DLP-системы,
- сетевое оборудование;
- прочие источники.

Количество источников событий возрастает с ростом организации, то есть с ростом числа серверов, автоматизированных рабочих мест, сетевого оборудования и прочих объектов инфраструктуры. Информация из различных источников хранится раздельно, имеет разные форматы, и, как следствие, никак не связана между собой. Для крупных организаций затруднительно обрабатывать достаточно быстро и эффективно такой поток событий ограниченным персоналом подразделения, ответственного за мониторинг.